di
Massimo F. Penco

La Posta Elettronica

Tecnica & Best Practice

Prefazione di Andrea Lisi

in appendice il testo integrale del nuovo Codice dell'Amministrazione Digitale

PuntoInformatico | Libri

Risk Mitigation Suite (RMS™)

Risk Mitigation Suite (RMS) - un insieme di prodotti ed utilità **GRATUITE**, per sensibilizzare gli utenti all'uso sicuro di Internet e dei propri sistemi. Questo enorme investimento economico del nostro gruppo, si è reso necessario per evitare

GlobalTrust Personal Secure Email

Incluso nella Suite RSM, la possibilità di avere un certificato S/MIME per la posta elettronica.

Potrete:

Codificare i messaggi di posta elettronica garantire **riservatezza** e **confidenzialità** dei dati inviati in rete utilizzando come strumento la posta elettronica;

Firmare digitalmente i messaggi di posta elettronica e relativi allegati con di garanzia di **autenticità, integrità e non ripudio** dei dati inviati in rete utilizzando come strumento la posta elettronica.

L' utilizzo del certificato S/MIME (posta elettronica certificata) permette di utilizzare le funzionalità di protezione presenti all' interno di Microsoft Outlook/Microsoft Outlook Express e di altri più comuni sistemi di posta elettronica: ***Firma digitale/Crittografa messaggi ed allegati.***

Gratis all'indirizzo:
https://www.globaltrust.it/modulo_reg_smime.asp
Maggiori informazioni:
http://www.globaltrust.it/products/prod_server/index.aspx

LA POSTA ELETTRONICA

TECNICA & BEST PRACTICE

Massimo F. Penco

PuntoInformatico | Libri

LA POSTA ELETTRONICA TECNICA & BEST PRACTICE

Di Massimo F. Penco

&

Associazione Cittadini di Internet
Via Caio Mario 8 00192 Roma
www.Cittadininternet.it www.cittadininternet.org
info@cittadininternet.org

Per La Versione E-BOOK questa è la Revisione: **1.10.00**

SOMMARIO
(LA POSTA ELETTRONICA TECNICA & BEST PRACTICE)

PREFAZIONE

Prof. Avv. Andrea Lisi[1] -

Chi vive senza follia non è così savio come crede. Mi è venuta in mente questa frase di François De La Rochefoucauld quando l'Amico Massimo Penco mi ha chiesto di scrivere una breve premessa per il suo ottimo volume sulla posta elettronica.
E certamente è presente un seme di sana follia in un volume che ha come assioma la considerazione che lo strumento e-mail non è sulla via del tramonto e che, anzi, sta rivivendo un suo personale successo all'interno dei più moderni social network.
Ma ancora più folli sono le modalità con cui questo testo viene oggi diffuso e veicolato, in forma dinamica, on line e cartacea. Un volume che, inoltre, si aggiorna nelle sue versioni elettroniche attraverso un'interazione possibile e costante con l'autore dello stesso.
Non è, forse, follia questa? Non si stanno capovolgendo le regole del mercato?
Il testo o è on line o è cartaceo, non può riassumere al suo interno entità contrapposte, direbbe il savio! Ma *il folle apre le vie che poi l'uomo savio percorre*. E Massimo Penco è abituato a farlo, stuzzicando la realtà (spesso indietro) con scenari inaspettati e futuribili.
E poi come fa un testo scritto, poi riversato su carta, ad aggiornarsi ogni giorno? *Verba volant, scripta manent*. E' "scritto" o "verbo" quanto leggiamo in forma dinamica nel mondo digitale?
Il testo è bello e rassicurante se si posa su carta, ma oggi vive ormai on line ed è giusto che viva la sua vita in modo autonomo e con aggiornamenti costanti, secondo quelle che sono le proprietà e i vantaggi della Rete.

---

[1] L'avv. Andrea Lisi è coordinatore del Digital&Law Department dello Studio Legale Lisi (www.studiolegalelisi.it) e Presidente della Associazione Nazionale per Operatori e Responsabili della Conservazione digitale dei documenti (ANORC). Già Docente di Informatica Giuridica nella Scuola di Professioni Legali, Facoltà di Giurisprudenza dell'Università del Salento, oggi è docente nella Document Management Academy, SDA Bocconi, Milano e di UniDOC- Progetto di formazione continua in materia di documentazione amministrativa, amministrazione digitale, delibere degli organi e documenti informatici - COINFO - Consorzio interuniversitario sulla formazione - Università degli Studi di Torino. Ha fondato il Centro Studi&Ricerche Scint www.scint.it e la prima banca dati sul diritto dell'informatica www.scintlex.it. È stato Direttore della "RIVISTA DI DIRITTO ECONOMIA E GESTIONE DELLE NUOVE TECNOLOGIE", Nyberg Editore, Milano e attualmente dirige la Collana "DIRITTO, ECONOMIA E SOCIETÀ DELL'INFORMAZIONE", Cierre Edizioni, Roma. Già componente del Comitato Scientifico nel Master in "DIRITTO DELL'INFORMAZIONE E DELL'INFORMATICA" presso l'Università di Messina (Direttore Prof. Trimarchi), oggi è nel Comitato Scientifico dell'Istituto Italiano per la Privacy (IIP) - http://www.istitutoitalianoprivacy.it, della Document Management Academy, SDA Bocconi, Milano, del DOCUBUSINESS (http://www.docubusiness.it), del Progetto e-HealthCare Forum (www.forumhealthcare.it), della Rivista Digital Document Magazine (edita da 4itGroup) e di varie riviste giuridiche telematiche ed è autore di diversi volumi e numerose pubblicazioni in materia di diritto delle nuove tecnologie.

Ha ragione Penco, quindi, a provocare e a generare impossibili commistioni tra realtà contrapposte?
Arthur Schopenhauer, un po' di anni fa, ci rivelò che *genio e follia hanno qualcosa in comune: entrambi vivono in un mondo diverso da quello che esiste per gli altri*.
Massimo Penco è, quindi, un genio o un folle?
Conosco l'ing. Penco da tempo e devo dirvi che non è facile rispondere a questa domanda. Per rispondere occorre sforzarsi di guardare oltre l'apparenza, oltre l'immediata percezione.
Osservare Massimo durante qualche conferenza nella sua irriverenza anti-istituzionale potrebbe spingerci facilmente a ritenerlo un folle. Eppure un genio come Jimi Hendrix ci rivela che *la pazzia è come il paradiso. Quando arrivi al punto in cui non te ne frega più niente di quello che gli altri possono dire. . . . . sei vicino al cielo*. E Massimo Penco, pur dissacrante nei modi e negli strumenti, rivela verità scomode.
Leonardo Da Vinci ci direbbe certamente che l'ing. Penco è folle perché vede e conosce più degli altri, perché *voi conoscerete la verità, e la verità vi renderà folli!*
E io, nella mia incerta lucidità, più volte l'ho seguito nelle sue battaglie sulla PEC. Condividendo, con la lente del giurista, idee, critiche, istanze.
E spesso aveva ragione. Sfogliavo la norma con attenzione e ne osservavo la sua evidente follia.
Non era Massimo il folle, ma il legislatore alcune volte rasentava la pazzia!
E poi è giusto ricordare che, *se da una parte ci sono più pazzi che savi e nel savio stesso c'è più pazzia che saggezza* (Nicolas De Chamfort), non si può non riconoscere che *non vi fu mai grande ingegno senza un po' di pazzia* (Lucio Anneo Seneca).
Insomma, Massimo Penco può piacere o non piacere nelle sue intemperanze, può a volte risultare poco diplomatico (anzi non lo è per nulla), ma spesso guarda lontano, oltre gli schemi abituali. E non so se questo volume possa portare alla saggezza o alla follia (come disse Petrarca), ma certamente non vi lascerà indifferenti.
Buona lettura!

CAPITOLO I. 1.0
POSTA ELETTRONICA: LE ORIGINI, L'EVOLUZIONE

LE ORIGINI

Questo importante tema richiederebbe un capitolo di approfondimento a parte, vista la complessità della materia. Pochi sanno che la posta elettronica comunemente definita come Electronic Mail (*e-mail*) è nata molto prima della nascita di Internet. Forse non tutti sanno che l'inventore o meglio il re-inventore del simbolo @ e dell'e-mail è **RAY TOMLINSON**[2] anche se ha origini più antiche – infatti @ era un'icona dei mercanti italiani (soprattutto veneziani), che la utilizzavano come abbreviazione commerciale dell'anfora, unità di peso e capacità dalle origini antichissime. La @, chiocciola, il più moderno simbolo della comunicazione umana ha cinquecento anni di vita e ha origini italiane. Come sostiene il prof. Giorgio Stabile, docente di Storia della Scienza presso l'Università La Sapienza di Roma, che ne ha trovato traccia negli scritti mercantili veneziani del cinquecento. Il simbolo @ rappresentava un'anfora e aveva il significato di unità di peso e di capacità. Da Venezia questo simbolo si era esteso in tutto il Mediterraneo. Nel 1972 l'ingegnere Ray Tomlinson, dovendo creare per la rete ARPANet, l'antenata di Internet, un sistema di posta interna, scelse la @[3] per separare il nome utente dal server negli indirizzi e-mail, ma

[2] **Raymond " Ray" Tomlinson** (Amsterdam, 1941) è un programmatore statunitense, inventore dell'e-mail nel 1971. Impegnato nello sviluppo di ARPANET, utilizzò questa procedura di invio di posta elettronica tra le diverse Università collegate attraverso questa rete. Ottenuto il bachelor in Scienza, al *Rensselaer Polytechnic Institute* di New York, nel 1963, entrò al MIT per specializzarsi in ingegneria elettrica, conseguendo la laurea nel 1965. Nel 1967 entra alla BBN Technologies che collabora al processo ARPANET, sviluppando il progetto di trasferimento dei files denominato *CPYNET*. Implementandolo, riuscì a progettare l'e-mail. Numerosi i premi ricevuti per l'importanza del suo lavoro nella crescita di internet.

[3] La @, anche detta **a commerciale**, e popolarmente nota come **chiocciola** o **chiocciolina**, conosciuta in inglese col nome **at**, è un carattere tipografico adoperato soprattutto per la posta elettronica. Grafica-

chi ne ha definito veramente il funzionamento si chiamava Jon Postel. Il simbolo @ in inglese si legge "at" o "at sign", ma ogni Nazione lo chiama "amichevolmente" in maniera diversa, in Italia *"Chiocciola"*.

LE PIETRE MILIARI DELLA POSTA ELETTRONICA

A partire dalla realizzazione del primo embrione di ARPANet[4], tutti i ricercatori, gli scienziati e gli studiosi coinvolti nella gestione dei primi nodi della rete hanno iniziato a sviluppare nuovi protocolli (regole di trasmissione dei dati) e nuovi servizi telematici, tra i quali il più noto è indubbiamente il servizio di posta elettronica (electronic mail o e-mail). Qui seguono le principali tappe storiche della posta elettronica.

1971 Ray Tomlinson, inventa un programma e-mail per spedire messaggi su reti distribuite.

1972 Ray Tomlinson modifica il programma e-mail per adattarlo ad ARPANet. Viene scelto il simbolo "@". Larry Roberts[5] (padre di ARPANet) scrive il primo programma di gestione delle e-mail (RD) per elencare, leggere selettivamente, archiviare, inviare e rispondere ai messaggi.

1973 SRI (NIC) pubblica la prima newsletter ARPANet News a marzo. Il numero degli utenti di ARPANet arriva a 2.000. Una ricerca dell'ARPA dimostra che le e-

mente, essa rappresenta una a stilizzata con attorno un ricciolo: da ciò derivano la somiglianza con il mollusco, di cui riproduce il guscio, e i nomignoli che essa possiede. Il codice binario (nel set ASCII a 8 bit) che serve ad identificarla è 01000000. Già in uso nel VII secolo d.C., presso i mercanti veneziani la @ era un segno grafico che rappresentava l'anfora, utilizzata allora come misura di peso e capacità. La si trova in un documento commerciale del 1536.[1] La @ nasce come unione stilizzata delle lettere "a" e "d" minuscole formanti la parola latina *ad* (cioè *"verso"*, nei moti a luogo). I popoli anglofoni modificarono il suo significato da *ad* a *at*, e quindi da *verso* a *presso* (grammaticalmente, da moto a luogo a stato in luogo) curvando l'asta della lettera *d* verso sinistra. La @ era presente nella macchina per scrivere Lambert del 1902 prodotta dalla Lambert Typewriter Company di New York e nell'IBM Selectric del 1961 e serviva ad abbreviare la frase commerciale "at a price of = al prezzo di". Nel 1963 venne inclusa nel set originale dei caratteri ASCII.

[4] **ARPANET** (acronimo di "Advanced Research Projects Agency NETwork", in italiano "rete dell'agenzia dei progetti di ricerca avanzata"), anche scritto **ARPAnet** o **Arpanet**, venne studiata e realizzata nel 1969 dal DARPA, l'agenzia del Dipartimento della Difesa degli Stati Uniti responsabile per lo sviluppo di nuove tecnologie ad uso militare. Si tratta della forma per così dire embrionale, dalla quale poi, nel 1983 nascerà Internet. Arpanet fu pensata per scopi militari statunitensi durante la Guerra Fredda, ma paradossalmente ne nascerà uno dei più grandi progetti civili: una rete globale che collegherà tutta la Terra.

[5] **Lawrence G. Roberts** (born 1937 in Connecticut[1]) received the Draper Prize in 2001[1] "for the development of the Internet" [2] along with Leonard Kleinrock, Robert Kahn, and Vinton Cerf. As a chief scientist at the Advanced Research Projects Agency, Roberts and his team created packet switching[1] and the ARPANet, which was the predecessor to the modern Internet.

	mail costituiscono il 75% di tutto il traffico su ARPA-Net.
1975	Steve Walker (Net Manager di ARPANet) crea la prima mailing list ARPANet, MsgGroup. Dopo poco tempo Einar Stefferud, (fondatore di Network Management Associates), ne diventa il moderatore. In quel periodo, una lista di fantascienza, SF-Lovers, diventò la lista non ufficiale più popolare. John Vittal, sviluppa MSG, il primo programma e-mail completo di funzioni di risposta, invio e archiviazione.
1976	La regina Elisabetta II di Inghilterra spedisce un'e-mail il 26 marzo dalla sede del Royal Signals and Radar Establishment (RSRE) a Malvern.
1977	Larry Landweber dell'Università del Wisconsin crea THEORYNET, il suo primo progetto che permette di fornire un servizio di e-mail a oltre 100 ricercatori di informatica, usando un sistema e-mail sviluppato in loco per funzionare con TELENET.
1979	Il 12 aprile, Kevin MacKenzie, (uno dei primi collaboratori allo sviluppo di ARPANet), spedisce un'e-mail a MsgGroup suggerendo di inserire all'interno del testo scritto dei simboli, per esprimere stati d'animo o emozioni. Pur facendo infuriare molti in quel periodo, i cosiddetti "emoticons" sono diventati in seguito estremamente popolari.
1982	Lo standard ufficiale dell'e-mail viene elaborato nel corso degli anni attraverso varie tappe, l'ultima delle quali è la RFC 821 dell'agosto 1982, con la quale si definisce SMTP (Simple Mail Transfer Protocol), il protocollo di trasmissione dei messaggi e-mail tuttora in uso. I protocolli che permettono l'invio e la ricezione delle e-mail sono: Simple Mail Transfer Protocol (SMTP), porta 25; Post Office Protocol 3 (POP3), porta 110; Internet Mail Access Control (IMAC), porta 143.
1989	Il numero di hosts supera le 100.000 unità. RIPE (Reseaux IP Europeens http://www.ripe.net) è creato (da service providers europei) per assicurare il necessario coordinamento tecnico e amministrativo per le opera-

	zioni del pan-European IP Network. Primi collegamenti fra un operatore commerciale di posta elettronica e Internet: MCI Mail attraverso la Corporation for the National Research Initiative (CNRI), e Compuserve attraverso la Ohio State University.
1994	Lo studio legale dell'Arizona Canter & Siegel inonda Internet di e-mail pubblicitarie (spamming) per una lotteria americana. Il traffico su NSFNET oltrepassa i 10 trilioni di bytes/mese.
1997	Vengono registrate 71.618 mailing lists (liste di distribuzione) alla directory di mailing list Liszt.
2001	Il worm Code Red e il virus Sircam entrano in migliaia di server e indirizzi e-mail, causando un picco vertiginoso di utilizzo della banda Internet e intrusioni nei sistemi di sicurezza.
2002-2009	La Posta Elettronica si è ulteriormente evoluta e perfezionata nel rispetto delle linee guida esistenti.

L'EVOLUZIONE

E' ormai invalso l'uso di servirsi di una "cosa" senza conoscerne esattamente le caratteristiche intrinseche: un tipico esempio è l'automobile. Nelle nuove tecnologie si apprendono gli elementi essenziali (vedi il cellulare) senza conoscere neanche i principi basilari con cui il sistema lavora, ma prima o poi succede qualcosa che costringe a saperne di più. Questa considerazione è alla base della nascita di questo breve libro sulla Posta Elettronica, ormai divenuto un sistema di comunicazione primario.
Questa spinta è stata rafforzata dall'avvento in Italia della PEC che ha senz'altro contribuito a complicare la situazione. La posta elettronica è nata, come tutti i sistemi di comunicazione umana, con l'intento di semplificare il sistema di comunicare in tutto il mondo, renderlo più efficiente e produttivo, libero e semplice da usare. Come ogni attività umana anche la posta elettronica è divenuta oggetto di un'infinità di usi illeciti ai quali si è dovuto porre rimedio. Si sente comunemente parlare di spam, di stalking, di phishing e, in tutte queste attività illecite, la posta elettronica è il mezzo in cui, in parte, queste attività vengono compiute. Tutto ciò non ha rallentato l'uso

della posta elettronica, che ormai è divenuto il sistema universale primario di comunicazione e usa diversi sistemi ed apparati per funzionare, non ultimi i telefoni cellulari.

IL FUNZIONAMENTO

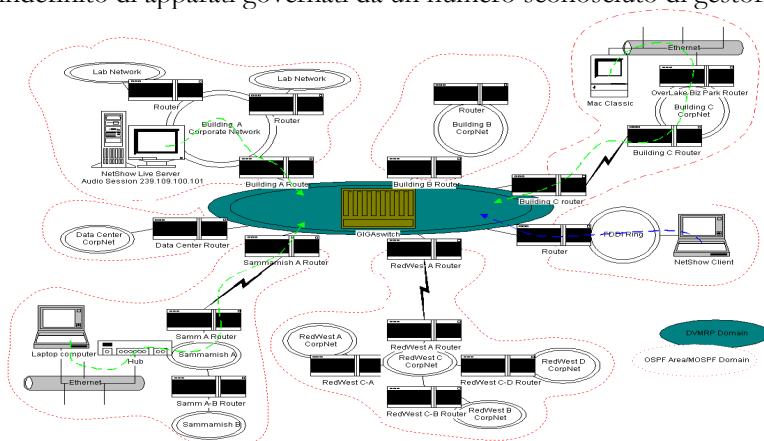
Per funzionare, la posta elettronica ha bisogno di un provider che fornisca ad un utente l'accesso ad Internet, gli assegna un identificativo che lo individua in modo univoco nella rete e in genere gli mette a disposizione anche una casella di posta elettronica, cioè uno spazio fisico nel server dove verranno automaticamente depositati i messaggi in partenza ed a lui diretti.

Per usufruire del servizio di posta elettronica abbiamo quindi bisogno di:

- Un computer o altri apparecchi predisposti come palmari e cellulari;
- Una casella di posta attivata da un Internet Service Provider (ISP)[6] con l'indirizzo relativo (es. nome@dominio.it);
- Un'interfaccia di posta elettronica Client o Browser.
- Il sistema di funzionamento della posta elettronica è abbastanza complesso ma, semplificando in modo banale, possiamo dire che un messaggio di posta elettronica può essere considerato come un testo scritto, *"file",* che viene scambiato tra mittente e destinatario, tramite server appositi.

  Non si deve cadere nell'errore che la trasmissione avvenga punto-punto come da immagine qui sotto similmente al fax:

[6] Un **Internet Service Provider** (termine mutuato dalla lingua inglese, che tradotto letteralmente in italiano significa "fornitore di servizi Internet"), in sigla **ISP**, anche abbreviato in **provider** se chiaro il contesto informatico, è una struttura commerciale o un'organizzazione che offre agli utenti (residenziali o imprese) servizi inerenti ad Internet, i principali dei quali sono l'accesso a Internet e la posta elettronica.

E' invece un sistema molto complesso che rappresenta, in un certo qual modo, cosa accade quando si accede ad Internet e si invia un messaggio di posta elettronica, come mostra la figura seguente lo stesso compie sconosciuta di percorsi, rimbalzando in un numero indefinito di apparati governati da un numero sconosciuto di gestori:

Architettura Complessa Per La Trasmissione Dati

CAPITOLO II. 2.0

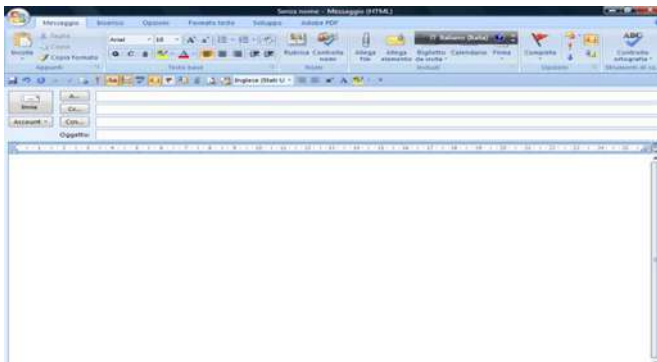
LA TECNICA, I PROTOCOLLI, GLI APPARATI

IL MESSAGGIO DI POSTA ELETTRONICA

Il messaggio di posta elettronica è composto da due parti principali:

1) intestazione del messaggio (header);
2) corpo del messaggio.

Intestazione del messaggio: come in una comune lettera il messaggio di posta elettronica contiene l'intestazione di chi spedisce l'e-mail, l'indirizzo di posta elettronica del mittente, DA: e l'indirizzo a cui viene inviato contrassegnato con la lettera A: .
L'indirizzo del destinatario/i a cui il messaggio viene inviato per conoscenza contrassegnato con l'acronimo **CC**.
L'indirizzo del destinatario/i a cui il messaggio viene inviato per conoscenza contrassegnato con l'acronimo CCn. usato qualora si voglia inviare il messaggio ad altri, senza però far vedere al destinatario principale la presenza di altri destinatari.

Si riporta per chiarezza la seguente figura.

Ecco un tipico esempio di intestazione (header) di un messaggio di posta elettronica: lo spazio bianco sotto l'intestazione è quello riservato al corpo del messaggio ed è molto importante capire

l'intestazione del messaggio ed il significato dei vari campi che sono in massima parte in lingua inglese.
Questa è l'intestazione standard che qualsiasi software client di posta elettronica mette automaticamente a disposizione dell'utente. L'header o intestazione di un messaggio, è in effetti qualcosa di più complesso, che con il progredire dei nuovi sistemi di posta elettronica offre una serie di importanti informazioni che rendono la stessa tracciabile in tutto il suo percorso, rendendo sempre più inutili tutte le prescrizioni dettate dalla PEC "made in Italy".

Come si può estrarre l'intestazione completa di un messaggio?
Ovviamente dipende dal sistema (software) usato, non è questa la sede per descrivere i vari sistemi, essendo sufficiente seguire le istruzioni (*help*) degli stessi. I risultati e le informazioni contenute nell'intestazione del messaggio differiscono profondamente in base a come il messaggio è stato inviato ed al formato scelto per l'invio. A prima vista sembreranno un serie di informazioni incomprensibili, ma analizzandole una ad una si capirà che non c'è nulla di più semplice per stabilire il percorso che un messaggio di posta elettronica compie. Questo enorme sforzo da parte di tutti coloro che hanno contribuito a stabilire dei protocolli standard per la posta elettronica, è diretto a dare un valore legale alla stessa, nel tentativo di renderla inattaccabile da eventuali intrusi od hacker e fornire, quanto meno, le informazioni necessarie per capire la genuinità e la provenienza di ogni singolo messaggio.
Al fine di rendere più realistica possibile l'intestazione del messaggio, nelle pagine che seguono, viene simulato il seguente caso:
Il messaggio firmato digitalmente attraverso l'uso di certificato x-509 inviato a più destinatari ed a più destinatari per conoscenza e per conoscenza nascosta, in modo da avere un'intestazione molto complessa: la prima, un messaggio di posta elettronica inviato, la seconda, un messaggio di posta elettronica ricevuto.
Da un primo esame superficiale sembrerebbe che il messaggio sia partito dal PC del mittente per giungere al PC dei destinatari. Come detto più volte, un messaggio di posta elettronica transita attraverso sistemi complessi che coinvolgono più di un server gestito da più di un ISP rimbalzando a volte tra una nazione ed un'altra. Questo accade anche quando i destinatari si trovano nella casa a fianco alla

nostra, in questi casi, ricostruire tutto il percorso, anche se complesso, è sempre possibile anche se può presentare delle difficoltà di non poco conto, soprattutto quando il messaggio viene gestito da ISP molto remoti e fuori dalla giurisdizione del Paese.

TIPICA INTESTAZIONE DI UN MESSAGGIO DI POSTA ELETTRONICA: INVIATO/RICEVUTO

Queste informazioni rimbalzano tra tutti i server in cui il messaggio transita, ogni modifica che viene fatta viene annotata garantendo l'autenticità ed immodificabilità, non solo del messaggio ma delle proprietà intrinseche dello stesso e dei suoi allegati.

PROPRIETA' HEADER	DATI IMMESSI DA UTENTE	DESCRIZIONE
Return-Path	scrivimi@rossi.it	Tracciamento di ritorno del messaggio
Delivered-To	cittadinInternet.org mpenco@cittadinInternet.org	Consegnato a
Received	(qmail 16876 invoked by uid 107); 3 Aug 2009 11:40:32 -0000	Ricevuto da: l'user identifier o **UID** è il numero che identifica univocamente un utente del sistema
X-Spam-Checker-Version	SpamAssassin 3.2.5 (2008-06-10) on hobbes.impulso.it	La versione del sistema antispamming residente nel server del provider di posta elettronica
X-Spam-Level		L'eventuale livello di spamming
X-Spam-Status	No, score=0.0 required=5.0 tests=none autolearn=disabled version=3.2.5	Lo status d'intervento del software anti-spamming in caso di messaggio spam
Received	from hermes.teseo.it (213.92.8.50) by vmx1 with ESMTPS (DHE-RSA-AES256-SHA encrypted); 3 Aug 2009 11:40:24 -0000	Il messaggio è stato ricevuto da un server denominato hermes.teseo.it identificato dal suo indirizzo IP. Il server ha provvedu-

		to anche ad identificare che il messaggio è firmato attraverso AES a 256 bit
Received-SPF	pass(vmx1:SPFrecordat pino.it designates 213.92.8.50 as permitted sender)	**SenderPolicyFramework** È il sistema per limitare gli abusi nella posta elettronica dove viene predeterminato il mittente autorizzato a spedire il messaggio ed altro ancora. Il sistema è piuttosto complesso ed ancora studiato da: http://www.openspf.org
Received	(qmail 27568 invoked from network); 3 Aug 2009 13:40:39 +0200	Data e ora di ricezione del messaggio stabilito dalla rete coinvolta nella gestione dello stesso
Received	from 93-43-156-184.ip92.fastwebnet.it (HELO pinocasa) (93.43.156.184) by hermes.teseo.it with SMTP; 3 Aug 2009 13:40:37 +0200	Qui vengono chiaramente indicate come i server dei provider si scambiano automaticamente informazioni relative al messaggio identificandosi con il proprio indirizzo IP. HELO è il sistema di mutuo riconoscimento dei server usato dal protocollo SMTP

Ed ecco un messaggio con la spiegazione delle sue proprietà, inviato a più destinatari con Protocollo S/MIME:

From: "Pino " scrivimi@pino.it

In questo caso il messaggio è stato inviato a più destinatari

To: "'Massimo F.Penco'" <mpenco@cittadininternet.org>, "'Marco '" <marco@marco.it>

Cc: "'Alberto \(alberto@banca.it\)'", References: Riferimenti univoci del messaggio !AAAAAAAAAAAYAA-AAAAAA-AJqvr/97qgtMorfeQLOmxhXCgAAAEAAAAJUlaZ0gnG9Moujl/FXUO2IBAAAAAA==@cittadinInternet.org le referenze univoche relative al messaggio

In-Reply-To:
!&!AAAAAAAAAAAYAAAAAAAAAJqvr/97qgtMorfeQLOmxhXCgAAAEAAAAJU-laZ0gnG9Moujl/FXUO2IBAAAAAA==@cittadinInternet.org
la risposta con codice univoco relativo al messaggio

Subject: R: LINK L'oggetto del messaggio

Date: Mon, 3 Aug 2009 13:40:08 +0200
la data e l'ora prelevata dall'ultimo server con l'adeguamento al fuso orario locale

Message:
ID:<!&!AAAAAAAAAAAYAAAAAAAAAJgFn/NeBRRJi7QWeNbLzJLCgAAAEAAAAH2+6P0GZYhFioA0GvLoes8BAAAAAA==@pino.it>
Il messaggio a questo punto viene fornito di un identificativo univoco che viene unito all'indirizzo del destinatario

MIME-Version:1.0 La versione del protocollo di trasmissione del messaggio

Content-Type:application/x-pkcs7-mime
l'applicazione con cui è stato firmato il messaggio

smime-type=signed-data

il tipo di firma del messaggio usata dal protocollo di trasmissione smime

name= "smime.p7m" il nome del file di firma e suo identificativo

Content-Transfer-Encoding: base64 Il codice di trasferimento del messaggio

Content-Disposition: attachment l'avviso che il messaggio contiene allegati

filename= "smime.p7m"
Il nome, protocollo del file usato per la firma del messaggio

X-Mailer: Microsoft Office Outlook 12.0
Il software usato per il servizio di posta elettronica

Thread-Index: A-coUG6TSCWUQHzvlTeSofK8/dGowkAAE0RCg identificativo dell'indicizzazione del messaggio di posta nel suo percorso

Content-Language: it
La lingua usata

Disposition-Notification-To: "Pino " scrivimi@pino.it
la disposizione data dal mittente a chi deve essere inviata l'e-mail

X-Antivirus: avast! (VPS 090802-0, 02/08/2009), Inbound message
Il tipo di Antivirus e versione nonché la data di aggiornamento e numero del data base usato dall'antivirus del messaggio in "transito"

X-Antivirus-Status: Clean
lo "status" del messaggio in questo caso "clean" privo di virus

Come si vede il messaggio e-mail non transita "solo" lungo il suo percorso, ma in compagnia di una fitta serie di informazioni, che lo rendono univoco e tracciabile. A tutto questo, hanno pensato i numerosi studiosi dei protocolli che permettono di usufruire di questo meraviglioso strumento, in cui la parte sicurezza è stata particolarmente curata.

I PROTOCOLLI DI BASE

Un aspetto essenziale, al fine della trasmissione di un messaggio, sono i protocolli di trasmissione dello stesso. Altro non sono che il modo in cui tutto il sistema fa sì che un messaggio parta, transiti ed arrivi a destinazione, cosa molto complessa, in quanto la posta elettronica deve operare in tutto il mondo ed i protocolli garantiscono l'assoluta interoperabilità degli stessi. Mancando questi, tutto il sistema non sarebbe compatibile con gli altri e non funzionerebbe. Gli studi e le ricerche si sono nel tempo particolarmente concentrati nel rendere sicuri i messaggi di posta elettronica attraverso protocolli e sistemi di trasmissione.

Eccone alcuni aspetti peculiari.

FUNZIONAMENTO DEI PROTOCOLLI

Può sembrare un argomento astruso, ma è strettamente necessario capire il funzionamento dei protocolli, altro non sono che dei sistemi per far funzionare e rendere interoperabili i vari apparati in tutto il mondo.

SPF (Sender Policy Framework)

Sender Policy Framework abbreviato in **SPF**[7] è un metodo per limitare gli abusi della posta elettronica in particolare nell'uso improprio del nome del mittente nei messaggi di posta elettronica. Si tratta di un protocollo tramite il quale è possibile definire *da dove* viene spedita la posta elettronica per una certa classe di mittenti.

Funzionamento del SPF

[7] **Sender Policy Framework** abbreviato in **SPF** è un metodo per limitare gli abusi del nome del mittente nei messaggi di posta elettronica. Si tratta di un protocollo tramite il quale è possibile definire *da dove* viene spedita la posta elettronica per una certa classe di mittenti.

Ciascun dominio[8] di posta elettronica[9] può pubblicare i criteri che contraddistinguono i mittenti che lo utilizzano. SPF definisce una varietà di metodi per indicare, direttamente o per riferimento, quali indirizzi IP possono essere usati dal mittente per spedire un'e-mail. Per esempio, è possibile indicare che i messaggi provenienti da *xxx*@esempio.it possano essere inviati soltanto da indirizzi IP europei. Dato che la maggior parte degli abusi, per evitare di essere legalmente perseguiti, sono commessi usando altri indirizzi IP, SPF potrebbe contrastare quel tipo di comportamento illegale.
I dati SPF, per definire la *policy,* sono pubblicati sul DNS[10] di ciascun dominio utilizzando il record SPF[11]. Il meccanismo funziona quindi come una DNSBL[12] distribuita. È importante notare che il blocco avviene *prima* della ricezione del testo messaggio, durante la fase iniziale del funzionamento del protocollo SMTP[13]. Dopo aver ricevuto un messaggio, un server di posta è tenuto a consegnarlo al destinatario oppure a notificare al mittente che il messaggio non viene consegnato. Dato che i mittenti dei messaggi abusivi sono, per l'appunto, abusivi, l'elaborazione dei metodi basati sui dati che si trovano all'*interno* del messaggio di posta è piuttosto limitata, dal punto di vista del gestore di un server di posta. Oltre a problematiche di ordine tecnico vi sono anche quelle di ordine giuridico come la privacy ecc, conseguentemente le possibilità che ha un ISP di controllare la messaggistica nei propri server è piuttosto ristretta.
Tutti i software maggiormente usati per i server di posta prevedono, in modo nativo o tramite *plugin*, di poter utilizzare *SPF (Sender Policy Framework)*[6]. L'adozione di *SPF* dipende quindi solo dalla volontà dei gestori di tali server. L'efficacia di *SPF* dipende dalla quantità di domini di posta che adottano questo protocollo ed è al momento limitata. Con riguardo specifico all'Italia, dove i gestori delle linee ADSL sfruttano al massimo la capienza di Internet dedicando agli utenti indirizzi IP variabili ad ogni connessione: questo purtroppo impedisce di fatto l'utilizzo del sistema SPF, qualora il fornitore di linea sia diverso dal provider/gestore del dominio.

[8] http://it.wikipedia.org/wiki/Dominio
[9] http://it.wikipedia.org/wiki/Posta_elettronica
[10] http://it.wikipedia.org/wiki/Domain_Name_System
[11] http://it.wikipedia.org/wiki/Tipi_di_record_DNS#SPF
[12] http://it.wikipedia.org/wiki/DNSBL
[13] http://it.wikipedia.org/wiki/Simple_Mail_Transfer_Protocol

SPF è nato nel 2003, dalle menti più brillanti che hanno contribuito allo sviluppo delle tecnologie Internet ed hanno apportato correzioni e aggiustamenti al progetto, a cui è seguita una fase di rapida diffusione.
Nel marzo 2004 IETF[14] lanciò il gruppo di lavoro MARID per promuoverne la standardizzazione. Subito dopo, il promotore ufficiale di SPF, POBox, si accordò con Microsoft per fondere in SPF la *CallerID*, in seguito divenuta poi *SenderID*: quest'ultimo è un progetto sostanzialmente diverso, in quanto si occupa dell'identificazione del mittente dopo che il messaggio è stato ricevuto.
Nel settembre 2004 il MARID[15] fu chiuso, prima che potesse pubblicare anche un solo RFC, a causa delle insanabili divergenze che erano sorte. Oggi SPF rimane un protocollo *sperimentale*, nondimeno, è adottato in Italia da banche di interesse nazionale, ditte e istituzioni che si preoccupano di sventare il phishing[16] tramite questo sistema.

- (**EN**)[17] Sito web del progetto OpenSPF[18]
- (**EN**)[16] RFC 4408[19] - Protocollo SPF per la sicurezza della posta elettronica.

IL PROTOCOLLO SMTP

Il *Simple Mail Transfer Protocol*, SMTP è il protocollo che permette di scambiare messaggi tra Host e si occupa di gestire quasi tutto il traffico e-mail su Internet. SMTP è un protocollo testuale, nel quale vengono specificati uno o più destinatari di un messaggio, verificata la loro esistenza, successivamente il messaggio viene trasferito.
Ai tempi in cui fu scritta la RFC 821 (1982), dove l'SMTP fu formalizzato definitivamente, erano stati esposti i migliori presupposti sul

---

[14] http://it.wikipedia.org/wiki/IETF La **Internet Engineering Task Force** è una comunità aperta di tecnici, specialisti e ricercatori interessati all'evoluzione tecnica e tecnologica di Internet. Ciò che differenzia IETF dagli Enti di standardizzazione più tradizionali è la sua struttura aperta: il lavoro viene svolto da gruppi di lavoro (*working groups*) che operano soprattutto tramite Mailing list, aperte alla partecipazione di chiunque sia interessato, e che si riuniscono tre volte l'anno. I gruppi di lavoro si occupano ciascuno di uno specifico argomento e sono organizzati in *aree* (protocolli applicativi, sicurezza, ecc...). Il motto di IETF è *Rough consensus and running code*, cioè *Consenso diffuso e codice funzionante*: le proposte di standard non vengono adottate con votazioni formali, ma viene richiesto, appunto, che ricevano un consenso generalizzato all'interno del gruppo di lavoro e che vi siano delle implementazioni funzionanti e diffuse. I gruppi di lavoro producono documenti denominati RFC (*Request For Comments*) che vengono sottoposti alla IESG (*Internet Engineering Steering Group*) per il loro avanzamento a standard ufficiale.
[15] http://datatracker.ietf.org/wg/marid/charter/
[16] http://it.wikipedia.org/wiki/Phishing
[17] http://it.wikipedia.org/wiki/Lingua_inglese
[18] http://www.openspf.org/
[19] http://tools.ietf.org/html/rfc4408

funzionamento del protocollo SMTP: doveva essere veloce, efficiente e soprattutto un protocollo indipendente, anche dal tipo di rete sottostante, indipendente anche da Internet. Nella pratica si è dovuto rivedere questo concetto onde evitare il collasso dei server SMTP, visto che i problemi di oggi circa l'abuso del servizio di posta di un server non erano certo quelli di allora.
Vediamo ora come avviene l'invio di un messaggio:

- Il programma di posta elettronica usato dall'utente invia il messaggio al proprio server (**A**) usando il protocollo SMTP, o può effettuare direttamente il collegamento con il server del destinatario senza utilizzare il proprio server, ciò non toglie che per arrivare a questo, il messaggio non rimbalzi in un numero imprecisato di server gestiti da un numero altrettanto indeterminato di provider.
- Il server trasferisce il messaggio al server del destinatario (**B**) utilizzando lo stesso protocollo.
    a) sulla base dell'indirizzo e-mail del destinatario, identifica il server **B** ed apre una connessione;
    b) identifica il nodo di rete da cui proviene la connessione (cioè il suo indirizzo IP) ed accetta la connessione, memorizza inoltre tale identificazione come parte iniziale del messaggio da ricevere;
    c) comunica lo username del destinatario;
    d) verifica la validità dell'indirizzo ed autorizza la trasmissione del messaggio;
    e) invia il messaggio e chiude la trasmissione;
    f) memorizza il messaggio in attesa che il reale destinatario si colleghi e ritiri il messaggio utilizzando un apposito protocollo (solitamente POP3 o IMAP).

Il destinatario preleva il messaggio dal proprio server e in base alla configurazione fissata potrà lasciare i messaggi nel server del provider per un periodo stabilito .
Affinché avvenga la consegna di un messaggio di posta elettronica dal mittente al destinatario, si utilizza normalmente un collegamento TCP attraverso la porta 25. Per associare il server a un dato nome di dominio (DNS) si usa un record denominato MX (Mail Exchange).
Un server SMTP "ascolta" sulla porta TCP/25 ed accetta connessioni sia da altri server che da client: quando si invia un messaggio, il

software si incarica di contattare il server SMTP del provider, che a sua volta cercherà l'SMTP del destinatario e recapiterà l'e-mail.
Infatti, ciò che normalmente viene identificato con l'etichetta "server della posta in uscita" non è altro che il server SMTP. In altre parole il protocollo SMTP definisce il formato dei messaggi da trasferire e il metodo relativo, l'host mittente usa comandi SMTP per mandare messaggi all'host ricevente.
Per inviare un messaggio, la prima cosa che deve fare il client SMTP è quella di inviare un comando al server SMTP specificando nel Reverse-Path o MAIL FROM:<elenco mittenti> il percorso che deve fare a ritroso il server SMTP per rispondere al client nel caso in cui dovesse ritornare al mittente un'e-mail contenente errori di spedizione. Il primo host nel Reverse-Path è in pratica la casella di posta del client (o colui che invia i comandi di posta).
Nel comando successivo, sempre il client SMTP, indica al server SMTP il Forward-Path o RCPT TO:<elenco destinatari> per l'inoltro del messaggio di posta. Il Forward di posta elettronica è il sistema attraverso il quale il server SMTP consegna il messaggio ad un destinatario diverso da quello indicato dal mittente; cosa possibile solo quando conosce all'interno del suo dominio il nome dell'indirizzo di posta o del dominio a cui deve inoltrare il messaggio. Conoscere il Forward-Path o il RCPT TO:<elenco host> è necessario per indicare il percorso che l'e-mail dovrà fare dal mittente al destinatario, una sorta di segnaletica stradale: il primo host o indirizzo di posta presente in questo elenco dovrà essere quello del server SMTP (o colui che riceve i comandi di posta) e se mancano sarà il server SMTP stesso ad aggiungerli automaticamente.
I due percorsi sono fondamentali per il Server SMTP, in quanto, attraverso il Reverse-Path è in grado di rispondere al client o all' host da cui riceve i comandi, mentre attraverso il Forward-Path è in grado di individuare i successivi server STMP a cui inviare comandi.
È a questo punto che interviene il relay. Il relay in pratica è l'operazione attraverso la quale il server SMTP toglie il primo host che trova nella coda del Forward-Path e lo aggiunge al primo posto nella coda del Reverse-Path o in altre parole, è il sistema attraverso cui il server SMTP invia i comandi ricevuti da un client SMTP (o da un server SMTP precedente), ad un server successivo, dello stesso dominio o appartenente ad un altro dominio. Con questa sostituzione può ora inviare i comandi al server SMTP successivo facendo fare

un passo in avanti al nostro messaggio di posta, e così via, fino a quando non si raggiunge la destinazione o la fine della coda nel Forward-Path. Il protocollo in questione definisce il formato dei messaggi da trasferire e il metodo relativo: l'host mittente usa comandi SMTP per mandare messaggi all'host ricevente, ovviamente descrivere tutti i passi che fa un messaggio di posta elettronica è molto complesso, ma nella realtà tutto questo avviene in pochi secondi.

Un metodo per verificare come funziona un server SMTP è usare un client Telnet:

1. Il client si connette alla TCP/25 del server, che risponde con un messaggio 220 <ready>.
2. Il client richiede l'inizio sessione con un comando HELO, seguito opzionalmente dal proprio nome completo di dominio (FQDN) o meglio il nome dell'host del client SMTP, e apre così la connessione. Il server risponde con 250 <OK>.
3. Il client specifica il mittente con mail from: <indirizzo>, il server: 250 <OK>.
4. Adesso il client identifica i destinatari con rcpt to:<indirizzo>, la risposta è ancora 250 <OK>.
5. Il client dichiara di essere pronto a trasmettere il vero messaggio con: data, risposta del server: 250 <OK>. Il messaggio viene trasmesso tramite caratteri ASCII a 7 bit.

Ricordiamo che inizialmente l'SMTP aveva delle limitazioni: era un protocollo testuale (basato sulla codifica ASCII), e non permetteva di trasmettere direttamente file binari, immagini ecc.. Furono poi sviluppati standard come il MIME per la codifica dei file binari ed il loro trasferimento attraverso SMTP. Attualmente i server SMTP supportano l'estensione 8BIT MIME che permette un trasferimento più agevole dei file binari, come se fossero file di testo. -

6. Una volta conclusa la trasmissione, il client invia la stringa di fine messaggio (di solito si tratta di un punto seguito da una riga vuota) e la sessione viene chiusa tramite il comando "quit". Ecco la sequenza relativa:

   C.Smtp1: HELLO host1
   S.Smtp1: HELLO host1
   C.Smtp1: MAIL FROM:<user1@host1>

S.Smtp1: ok.
C.Smtp1:RCPT
TO:<@host2,@host3:user4@host4,user5@host5>
S.Smtp1: ok.
C.Smtp1: DATA:
Prova messaggio di posta
S.Smtp1: ok.
C.Smtp1: QUIT

[Le righe inviate dal client sono precedute da "C:", mentre quelle inviate dal server da"S:"].

Nell'esempio il client ***Smtp1*** coincide con ***host1***, mentre non necessariamente il server Smtp1 deve essere uguale al primo host presente nel Forward-Path, pertanto potrebbe essere S.Smtp1=host2, ma anche non esserlo.
Per comodità supponiamo che il server Smtp1 sia host2, ma se così non fosse stato si sarebbe semplicemente allungata la coda nel Reverse-Path: il server Smtp1 avrebbe aggiunto il proprio dominio all'inizio della coda e così avrebbero fatto tutti gli altri server Smtp, qualora non ci fosse stata corrispondenza tra il domino del server Smtp che riceve i comandi ed il primo host presente nella coda del Forward-Path. Neanche il client Smtp1 dovrà necessariamente essere uguale all'host1, del resto il primo host del Reverse-Path indica semplicemente il primo indirizzo a cui restituire eventuali mail contenenti errori.
A questo punto il server Smtp1 inizierà una comunicazione con il server Smtp2 che coincide con il dominio @host3 come segue :

S.Smtp1: HELLO host2
S.Smtp2: HELLO host2
S.Smtp1: MAIL FROM:<@host2,user1@host1>
S.Smtp2: ok.
S.Smtp1: RCPT TO:<@host3:user4@host4,user5@host5>
S.Smtp2: ok.
S.Smtp1: DATA:
Prova messaggio di posta
S.Smtp2: ok.
S.Smtp1: QUIT

A questo punto il server Smtp2 che coincide con host3 consegna il messaggio all'utente user4@host4 (evidentemente sa come fare il forward di questo messaggio all'host4), in alternativa l'host3 avrebbe iniziato una comunicazione SMTP con l'host4, oppure, se non in grado, avrebbe restituito un errore a user1@host1 grazie alle informazioni contenute nel Reverse-Path, i server avrebbero saputo come raggiungerlo a ritroso.

S.Smtp2: HELO host3
S.Smtp3: Hello
S.Smtp2: MAIL FROM:<@host3,@hot2,user1@host1>
S.Smtp3: ok.
S.Smtp2: RCPT TO:<user5@host5>
S.Smtp3: ok.
S.Smtp2: DATA:
Prova messaggio di posta
S.Smtp3: ok.
S.Smtp2: QUIT

A questo punto è stato recapitato il messaggio all'ultimo destinatario presente nella coda.
Ora sicuramente una domanda è d'obbligo: l'SMTP è sicuro? Una delle limitazioni del protocollo SMTP originario era che non gestiva l'autenticazione dei mittenti. Per ovviare a questo problema è stata sviluppata un'estensione chiamata SMTP-AUTH. Nonostante questo, lo spam rimane ancor oggi un grave problema. Tuttavia, non si ritiene praticabile una revisione radicale del protocollo SMTP per via del gran numero di implementazioni del protocollo attuale. Ciò nonostante per limitare lo spam, un server SMTP accetta posta solo per gli utenti del proprio dominio, rifiutando il "relay".
Una volta che il server SMTP del provider ha ricevuto il messaggio, contatta il server SMTP incaricato della ricezione e gli trasmette l'e-mail.
SMTP è un protocollo che permette soltanto di inviare messaggi di posta, ma non di richiederli ad un server: per fare questo il client di posta deve usare altri protocolli, quali il POP3 (*Post Office Protocol*), l'IMAP (*Internet Message Access Protocol*).

GLI STANDARD DI TRASMISSIONE DELLA POSTA ELETTRONICA

L'esigenza di avere un altro protocollo di trasmissione delle e-mail si fece sentire per due principali ragioni:

- la sicurezza;
- la necessità di inviare messaggi anche con grafica ed altri formati multimediali od in formato diverso dal solo testo ed altro ancora.

PROTOCOLLO MIME

- MIME[20] consente anche di avere diversi contenuti nello stesso messaggio (*multipart message body*) e su questo meccanismo si basa la possibilità di aggiungere allegati (*attachments*) ai messaggi di posta elettronica
- La codifica MIME prevede la notificazione di due parametri (ossia intestazioni SMTP):
    - Content-Type: per notificare il tipo di dati (nella forma type/subtype)

    - Content-Transfer-Encoding: è il sistema per definire il meccanismo di codifica nella trasmissione dei messaggi

Type	Subtype	Descrizione
text	plain	testo libero
	html	testo in formato HTML
image	gif	immagine in formato GIF
	jpeg	immagine in formato JPEG
	png	immagine in formato PNG
audio	basic	suono udibile

[20] Il **Multipurpose Internet Mail Extensions** (**MIME**) è uno standard di Internet che definisce il formato delle e-mail. Una buona parte delle e-mail che circolano su Internet sono spedite via SMTP in formato MIME. Le e-mail sono così, strettamente connesse agli standard SMTP e MIME, spesso chiamate e-mail SMTP/MIME. Oltre che per il contenuto delle e-mail, la tipizzazione MIME è adoperata anche nel protocollo HTTP e nel codice HTML.

video	mpeg	filmato in formato MPEG
application	octet-stream	sequenza di byte che non viene interpretata dallo *user agent*
	postscript	documento stampabile in formato *Postscript*
message	rfc822	messaggio che rispetta le specifiche SMTP di base
	partial	messaggio che è stato spezzato in più parti per la trasmissione
	external-body	il messaggio stesso deve essere recuperato dalla rete
Multipart - nel valore viene anche espresso un codice unico che fa da divisore (boundary) tra le differenti parti del messaggio; ogni parte ha propri Content-Type e Content-Transfer-Encoding	mixed	le parti sono indipendenti tra loro
	alternative	lo stesso messaggio in diversi formati
	parallel	le parti devono essere viste simultaneamente
	digest	ogni parte è un messaggio completo che rispetta le specifiche RFC 822

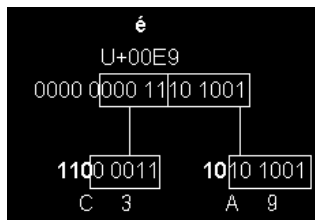
- Nel caso di Content-Type testuale (text/plain o text/html) nel valore del parametro viene anche specificato l'attributo charset;

- I valori di Content-Transfer-Encoding più comuni sono:
    - 7bit (*default*)
    - 8bit
    - base64
    - binary
    - quoted-printable

Confronto tra quoted-printable e base 64 di un testo codificato in UTF-8[21]

[21] **UTF-8** (**U**nicode **T**ransformation **F**ormat, **8** bit) è una codifica dei caratteri Unicode in sequenze di lunghezza variabile di byte, creata da Rob Pike e Ken Thompson. UTF-8 usa gruppi di byte per rappresentare i caratteri Unicode, ed è particolarmente utile per il trasferimento tramite sistemi di posta elettronica a 8-bit. UTF-8 usa da 1 a 4 byte per rappresentare un carattere Unicode. Per esempio un solo byte è necessario per rappresentare i 128 caratteri dell'alfabeto ASCII, corrispondenti alle posizioni Unicode da U +0000 a U+007F. Quattro byte possono sembrare troppi per un solo carattere; tuttavia questo è richiesto solo per i caratteri che stanno fuori dal *Basic Multilingual Plane*, generalmente molto rari. Inoltre anche UTF-16 (la

- Consideriamo la parola ola f cese *Résumé*
- Il carattere é (*code point value* U+00E9) in UTF-8 occupa due byte che valgono 0xC3 0xA9
- ecco il confronto tra i due *transfer encoding:*

UTF-8 per *code point values* compresi nell'intervallo da U+0080 a U+07FF

Content-Type: text/plain; charset=utf-8
Content-Transfer-Encoding: quoted-printable

R=C3=A9sum=C3=A9

Content-Type: text/plain; charset=utf-8

Content-Transfer-Encoding: base64
...
UsOpc3Vtw2k=

Esempio di utilizzo di Base64 in un allegato di posta elettronica

Specifica il tipo ed il sottotipo di dati contenuti nel messaggio (MIME type), in modo che il software che riceve il messaggio possa immediatamente capire come sono codificati i dati ricevuti.

Questo campo ha la forma:

Content-Type: tipo/sottotipo;[parametro]

Dove *tipo* specifica la forma generale dei dati, mentre *sottotipo* specifica il particolare tipo dei dati trasmessi. Il campo *parametro* è opzionale.

Il *tipo* può essere uno di quelli riportati di seguito.

text

principale alternativa a UTF-8) richiede quattro byte per questi caratteri. Quale sia più efficiente, UTF-8 o UTF-16, dipende dall'intervallo di caratteri utilizzati, e l'uso di algoritmi di compressione tradizionali riduce in maniera significativa la differenza tra le due codifiche. Per brevi brani di testo, su cui gli algoritmi di compressione tradizionali non sono efficienti e una ridotta occupazione di memoria è importante, si potrebbe utilizzare lo Schema di compressione standard per Unicode. La IETF (*Internet Engineering Task Force*) richiede che tutti i protocolli Internet identifichino la codifica dei caratteri utilizzata e che siano in grado di utilizzare almeno UTF-8.

Può essere utilizzato per rappresentare informazioni in forma testuale, scritte secondo un certo linguaggio. Un *sottotipo* per *text* è *plain*, che indica un testo non formattato, un altro è *richtext*, usato per testi con una semplice formattazione. Un *parametro* usato per i messaggi *text* è *charset*, che è usato per indicare il set di caratteri utilizzato.
Ad esempio, per la posta elettronica in Internet, il campo Content-Type assume la forma:
Content-Type: text/plain; charset=us-ascii
Nel caso non sia specificato il *parametro*, viene usato come default il set di caratteri *US-ASCII*[22].

multipart
E' utilizzato per indicare documenti che si compongono di più parti, ognuna contenente un tipo diverso di dati. Il *sottotipo* principale è *mixed*, usato per indicare che le varie parti del documento sono tra loro indipendenti e visualizzate in serie. Un altro *sottotipo* è *alternative*, usato per documenti in cui sono contenuti gli stessi dati in formati diversi; ogni parte è una versione alternativa delle altre ed il programma ricevente visualizzerà la parte che più si adatta alle sue caratteristiche. Altri *sottotipi* sono *digest* e *parallel*: *digest* converte le parti indicate con *text/plain* in *message/rfc822* (vedi più avanti il tipo *message*), mentre *parallel* viene usato quando tutte le parti del documento devono essere rappresentate per poter essere lette simultaneamente (in un sistema - hardware e software - che è capace di farlo, altrimenti le parti vengono presentate in serie successive). Un *parametro* molto importante per i documenti *multipart* è *boundary*, utilizzato per specificare il confine che separa le varie parti del documento; *boundary* è costituito da una stringa generica che viene poi inserita tra una parte e la successiva, facendola precedere dai caratteri "--". La stringa si deve trovare anche alla fine dell'ultima parte del documento e, in quest'ultimo caso, i caratteri "--" devono essere sia all'inizio della stringa, che alla fine di essa.
Un documento *multipart* avrà quindi la seguente struttura:

---

[22] È un sistema di codifica dei caratteri a 7 bit[1] comunemente utilizzato nei calcolatori, proposto dall'ingegnere dell'IBM Bob Bemer nel1961, e successivamente accettato come standard dall'ISO (ISO 646). Per non confonderlo con le estensioni a 8 bit proposte successivamente, questo codice viene talvolta riferito come **US-ASCII**.

Content-Type: multipart/mixed; parameter=Fine Parte

PRIMA PARTE

--Fine Parte

SECONDA PARTE

--Fine Parte—

application

Viene usato per trasmettere una certa applicazione dei dati in forma binaria, quindi per realizzare una trasmissione di file utilizzando la posta elettronica. Un *sottotipo* è *octet-stream* in cui si devono trasmettere dati binari senza interpretarli (vengono salvati in un file); Un altro è: *ODA* e *PostScript*, usati rispettivamente per trasportare documenti ODA (in questo caso il documento contiene informazioni codificate secondo lo standard (Office Document Architecture) e Postscript.

message

E' utilizzato per indicare un messaggio di posta elettronica scritto secondo il formato RFC 822. Il s*ottotipo* principale è appunto *rfc822*, altrimenti usa la funzione *partial*, per permettere la frammentazione del messaggio quando le sue dimensioni sono troppo grandi, oppure *External-body*, per indicare che il messaggio non è incluso e sono indicati dei parametri che descrivono come reperirlo.

image

E' utilizzato per trasmettere dati costituenti un'immagine. Il tipo di immagine (GIF, JPEG, ecc.) sarà poi specificato nel *sottotipo* tramite l'estensione del file; avremo quindi: *gif*, *jpeg*, ecc..

audio

Viene usato per trasmettere dati di un file audio. Attualmente l'unico *sottotipo* usato è *basic* ed ha validità generale.

video

Usato per trasmettere dati costituenti immagini in movimento, possibilmente con un audio associato. Il *sottotipo* usato è legato alla codifica del video (ad esempio, *mpeg*).

Content-ID
Identifica il messaggio in modo univoco (opzionale).

Content-Transfer-Encoding
Specifica un modo accessorio di codifica dei dati a quello principale, utilizzato per permettere loro di passare attraverso tutti i meccanismi di trasporto della posta elettronica, i quali potrebbero avere delle limitazioni nel set di caratteri ammessi (questa codifica aggiuntiva deve essere applicata ai dati prima della loro trasmissione). I documenti, per essere trasportati in rete, necessitano di un'ulteriore codifica chiamata *content-transfer-encoding* dove viene specificato qual è la relazione tra i dati nella loro forma originale ed il formato con cui vengono trasmessi. La maggioranza dei documenti può così essere trasportata nella rete senza problemi, anche nel caso in cui i dati debbano attraversare una rete conforme soltanto allo standard RFC 822 e non alle sue successive versioni (come MIME); un esempio è un sistema di posta compatibile col protocollo SMTP (*Simple Mail Transfer Protocol*), in cui è necessario che il documento venga opportunamente codificato in caratteri ASCII, a 7 bit, con non più di 1000 linee. Il campo *Content-Transfer-Encoding* è appunto usato per specificare come possono essere manipolati i dati per essere trasportati in rete; in esso viene specificato un meccanismo, invertibile, per trasformare il documento originario e non ha alcuna influenza sul tipo dei dati trasportati.

I valori di *Content-Transfer-Encoding* sono: 7bit, 8bit, binary, quoted-printable, base64. Il loro significato è il seguente:

- ***7bit, 8bit, binary:*** questi valori stanno a significare che nessuna operazione di codifica è stata effettuata sul contenuto del messaggio e, allo stesso tempo, forniscono un’indicazione sul tipo dei dati contenuti nel messaggio stesso (quindi forniscono un'indicazione sul tipo di codifica che potrebbe rendersi necessaria per trasmettere il messaggio in determinati sistemi di trasmissione. Il valore "7bit" significa che in questo caso i dati possono essere rappresentati in gruppi di sette bit, ognuno dei quali deve essere contenuto obbligatoriamente nel set di caratteri ASCII; questo

è anche il valore assunto come default se il campo non viene specificato. Il valore "8bit" significa che possono essere presenti caratteri non appartenenti al set ASCII; cioè, suddividendo il messaggio in linee di 8 bit ciascuna e associando ad ogni linea un carattere ASCII, si possono ottenere delle sequenze di caratteri apparentemente senza significato o comunque non previsti. Il valore "binary" indica che il contenuto del messaggio è in formato binario (un'immagine, un file audio, ecc.). La differenza tra "8bit" e "binary" può sembrare irrilevante ma può assumere grande significato in quei sistemi di trasferimento dati che non sono conformi alle restrizioni della RFC 821.

- ***quoted-printable:*** questo valore significa che un'operazione di codifica è già stata applicata ai dati, in modo da trasformare il messaggio in una sequenza di caratteri ASCII, se il messaggio originario era già costituito da un testo ASCII, questa codifica lo lascia sostanzialmente inalterato. Lo scopo principale di questa codifica è di mettere i dati in un formato che difficilmente subirà delle trasformazioni da parte dei vari sistemi che è costretto ad attraversare, prima di giungere a destinazione.
- ***base64:*** questo valore significa che sui dati è stata effettuata un'operazione di codifica, detta base64; con questa operazione il messaggio viene trasformato in una sequenza di caratteri appartenenti ad un sottogruppo del set di caratteri ASCII (le lettere maiuscole da "A" a "Z", quelle minuscole da "a" a "z", I numeri da"0" a "9", il carattere "+" ed il carattere "\|"). In questo modo, ogni carattere codificato può essere rappresentato con sei bit. L'operazione di codifica consiste nel suddividere la sequenza dei bit in ingresso (il messaggio) in gruppi di 24 bit; ogni gruppo di 24 bit viene diviso in quattro gruppi di sei bit, ad ognuno dei quali si associa il corrispondente carattere ASCII appartenente al sottogruppo specificato.
- ***x-token:*** viene usato per specificare uno schema di codifica esterno, non standard, scelto da chi trasmette il messaggio (*token* coinciderà col nome dato a questa codifica); si deve fare attenzione al fatto che questa codifica deve essere nota

anche a chi riceve il messaggio, in modo che questo possa essere ricostruito correttamente.

MIME

Per garantire che un messaggio di posta elettronica viaggi attraverso qualsiasi server SMTP, è necessario che si rimanga nell'ambito dei soli 7bit, oltre al fatto di avere un limite alla lunghezza delle righe e non poter trasmettere altro che testo in formato ASCII[23].
La necessità di scrivere in lingue differenti dall'inglese e di poter trasmettere informazioni diverse dal solito testo puro e semplice, ha fatto nascere lo standard multimediale MIME (*Multipurpose Internet Mail Extentions*).
Con le estensioni multimediali MIME è possibile definire come deve essere interpretato il contenuto di un messaggio di posta elettronica, che così può essere codificato in modo particolare, per trasportare anche informazioni diverse dal solo testo ASCII puro, rispettando i limiti tradizionali dei sistemi di trasporto dei messaggi. In pratica, per quanto riguarda la lingua italiana, non ci possono essere lettere accentate. MIME (Multipurpose Internet Mail Extensions) è uno standard generico per il formato dei documenti scambiati sulla rete Internet tramite posta elettronica, news, ecc. (standard generico significa che prevede tutte le possibili funzionalità per la trasmissione dei documenti).
Inizialmente il protocollo per la rappresentazione dei documenti di posta elettronica (e-mail) era definito nel documento RFC (Request For Comments) 822, del 1982; in questo documento veniva specificato il formato per i messaggi di posta e ci si limitava a messaggi esclusivamente di tipo testo ASCII, senza alcun riferimento a messaggi di altro tipo (ad esempio, le immagini). Nel giugno 1992 è stato

[23] **ASCII** è l'acronimo di **A**merican **S**tandard **C**ode for **I**nformation **I**nterchange (ovvero *Codice Standard Americano per lo Scambio di Informazioni*), pronunciato in inglese *askey* /ˈæski/, mentre in italiano è comunemente pronunciato *asci* /ˈaʃʃi/. È un sistema di codifica dei caratteri a 7 bit[1] comunemente utilizzato nei calcolatori, proposto dall'ingegnere de ll'IBM Bob B emer nel 1961, e s uccessivamente ac cettato c ome standard dall'ISO (ISO 646). Per non confonderlo con le estensioni a 8 bit proposte successivamente, questo codice viene talvolta riferito come **US-ASCII**. Alla specifica iniziale basata su codici di 7 bit fecero seguito negli anni molte proposte di estensione ad 8 bit, con lo scopo di raddoppiare il numero di caratteri rappresentabili. Nei PC IBM si fa, per l'appunto, uso di una di queste estensioni, ormai standard di fatto, chiamata *extended ASCII* o *high ASCII*. In questo ASCII esteso, i caratteri aggiunti sono vocali accentate, simboli semigrafici e altri simboli di uso meno comune. I caratteri *extended ASCII* sono codificati nei cosiddetti codepage.

presentato un nuovo documento, l'RFC 1341 (i documenti RFC possono essere trovati ai seguenti indirizzi: "ftp://ds.internic.net/rfc", "http://cwis.auc.dk/rfc/rfc"), nei quali viene descritto lo standard MIME. In RFC 1341 vengono presentati i meccanismi per superare le limitazioni contenute in RFC 822; viene specificato come definire il formato sia di messaggi testuali (ASCII e non) sia di messaggi multimediali (cioè contenenti video, suoni, immagini, ecc.). Una delle principali limitazioni del protocollo descritto in RFC 822 si ha nel fatto che il contenuto dei messaggi è limitato a simboli (caratteri) di 7 bit; questo impone che ogni messaggio non costituito da solo testo ASCII, debba essere convertito in questo formato prima di essere inviato in rete. Per risolvere questo problema è stato proposto il documento RFC 1341.
Quando due programmi dialogano tra loro, attraverso la rete Internet, (uno invia un file e l'altro lo riceve), il programma che invia il file deve specificarne il tipo secondo lo standard MIME; in questo modo il programma che riceve i dati può capire come trattarli.
Con lo standard MIME è possibile inserire in un qualsiasi messaggio di e-mail, oltre al testo, anche i file contenenti immagini, segnali audio e video; il software che gestisce la posta non si preoccupa del contenuto del messaggio, è l'utilizzatore finale a preoccuparsi della sua opportuna decodifica in base alle specifiche di tipo inserite nel messaggio stesso.
In MIME, come descritto in RFC 1341, vengono introdotti dei meccanismi che permettono di risolvere i problemi di RFC 822, senza introdurre delle incompatibilità con i documenti scritti secondo il vecchio standard.

Un documento MIME contiene una testata in cui si trovano i seguenti campi:

MIME version

Identifica la versione dello standard MIME usato nel messaggio. Questo permette di indicare se un messaggio è conforme allo standard, in modo tale che il software che lo riceve possa distinguerlo da quei messaggi scritti secondo il vecchio standard (in cui questo campo è assente).

Content-Type
Specifica il tipo ed il sottotipo di dati contenuti nel messaggio (MIME type), in modo che il software che riceve il messaggio possa immediatamente capire come sono codificati i dati ricevuti.
Questo campo ha la forma:
Content-Type: tipo/sottotipo;[parametro]
Dove *tipo* specifica la forma generale dei dati, mentre *sottotipo* specifica il particolare tipo dei dati trasmessi. Il campo *parametro* è opzionale. Il *tipo (type)* può essere uno di quelli riportati di seguito.

text
Può essere utilizzato per rappresentare informazioni in forma testuale, scritte secondo un certo linguaggio. Un *sottotipo* per *text* è ***plain***, che indica un testo non formattato, un altro è ***richtext***, usato per testi con una semplice formattazione. Un *parametro* usato per i messaggi *text* è ***charset***, che è usato per indicare il set di caratteri utilizzato.
Ad esempio, per la posta elettronica in Internet, il campo Content-Type assume la forma:
Content-Type: text/plain; charset=us-ascii
Nel caso non sia specificato il *parametro*, viene usato come default il set di caratteri *US-ASCII.*

multipart
E' utilizzato per indicare documenti che si compongono di più parti, ognuna contenente un tipo di dati diverso.
Il *sottotipo* principale ***mixed***, è usato per indicare che le varie parti del documento sono tra loro indipendenti e visualizzate in serie.
Un altro *sottotipo* è ***alternative***, usato per documenti in cui sono contenuti gli stessi dati in formati diversi; ogni parte è una versione alternativa delle altre ed il programma ricevente visualizzerà la parte che più si adatta alle sue caratteristiche.
Altri *sottotipi* ancora sono: *digest* e *parallel.* D***igest*** converte le parti indicate con *text/plain* in *message/rfc822* (vedi più avanti il tipo *message*), mentre ***parallel*** viene usato quando tutte le parti del documento devono essere rappresentate simultaneamente (su un sistema - hardware e software - che è capace di farlo, altrimenti le parti vengono presentate in serie).

Un *parametro* molto importante per i documenti *multipart* è ***boundary***, utilizzato per specificare il termine che separa le varie parti del documento; *boundary* è costituito da una generica stringa che viene poi inserita tra una parte e la successiva, facendola precedere dai caratteri "**--**". La stringa si deve trovare anche alla fine dell'ultima parte del documento e, in quest'ultimo caso, i caratteri "--" devono essere sia all'inizio della stringa sia alla fine di essa.

Un documento *multipart* avrà quindi la seguente struttura:
Content-Type: multipart/mixed; parameter=FineParte

PRIMA PARTE
--FineParte
SECONDA PARTE
--FineParte--

application

Viene usato per trasmettere una certa applicazione dei dati in forma binaria, quindi per realizzare una trasmissione di file utilizzando la posta elettronica. Un *sottotipo* èn ***octet-stream*** in cui si devono trasmettere dati binari senza interpretarli (vengono salvati in un file); poi si hanno ***ODA*** e ***PostScript***, usati rispettivamente per trasportare documenti ODA (in questo caso il documento contiene informazioni codificate secondo lo standard Office Document Architecture) e Postscript.

message

E' utilizzato per indicare un messaggio di posta elettronica scritto secondo il formato RFC 822. Il s*ottotipo* principale è appunto ***rfc822***, altrimenti si ha ***partial***, per permettere la frammentazione del messaggio quando le sue dimensioni sono troppo grandi, oppure ***external-body***, per indicare che il messaggio non è incluso e sono indicati dei parametri che descrivono come reperirlo.

image

E' utilizzato per trasmettere dati costituenti un'immagine. Il tipo di immagine (GIF, JPEG, ecc.) sarà poi specificato nel *sottotipo* tramite l'estensione del file; avremo quindi: *gif*, *jpeg*, ecc..

audio
Viene usato per trasmettere dati di un file audio. Attualmente l'unico *sottotipo* usato è ***basic*** ed ha validità generale.

video
Usato per trasmettere dati costituenti immagini in movimento, possibilmente con un audio associato. Il *sottotipo* usato è legato alla codifica del video (ad esempio, ***mpeg***).

Esempio di documento MIME
Quello riportato di seguito è un esempio di documento *multipart*. In esso si hanno cinque parti che vengono visualizzate in serie: due parti sono testo di tipo *text/plain (solo testo)*, poi si ha una parte *multipart/parallel*, in cui viene visualizzata un'immagine accompagnata da un audio; successivamente, si ha ancora del testo di tipo *text/rich text* e, infine, un messaggio scritto in un set di caratteri diverso dall'ASCII.

MIME-Version: 1.0
From: [il nome del mittente ed il suo indirizzo di e-mail]
Subject: Oggetto: ad esempio MIME-Multipart
Content-type: il tipo del contenuto multipart/mixed; boundary=termine-1
[Questa area è riservata al testo del messaggio]
--termine-1
[Ancora testo; la linea vuota tra "--termine-1" e l'inizio del testo significa che non si è specificato il tipo di testo (con *Content-Type*) e quindi, viene preso come default un testo scritto in caratteri US-ASCII. Il testo poteva comunque essere specificato, come viene fatto nella parte successiva]
--termine-1
Content-type: text/plain; charset=US-ASCII
[Ancora testo; risulta evidente che questa parte avrebbe potuto essere inclusa nella precedente]
--termine-1
Content-type: multipart/parallel; boundary=termine-2
--termine-2

Content-type: audio/basic
Content-Transfer-Encoding: base64
[dati audio]
--termine-2
Content-type: image/gif
Content-Transfer-Encoding: base64
[dati immagine]
--termine-2--
--termine-1
Content-type: text/richtext
Testo <bold><italic>richtext</italic></bold>.
--termine-1
Content-type: message/rfc822
From: [qui va il mittente scritto in caratteri US-ASCII]
Subject: [qui va il soggetto del messaggio, scritto in caratteri US-ASCII]
Content-type: text/plain; charset=ISO-8859-1
Content-Transfer-Encoding: Quoted-printable
[testo scritto col set di caratteri ISO-8859-1]
--termine-1—

Si può notare come la stringa usata come *boundary* viene sempre preceduta dai caratteri "**--**"; gli stessi caratteri vengono posti alla fine del *boundary* solo quando questo indica la fine del documento *multipart*.

GLI APPARATI HARDWARE PER L'USO DELLA POSTA ELETTRONICA

Anche se può sembrare banale, ma estremamente utile, diamo uno sguardo agli apparati, ovverosia l'hardware occorrente, per l'invio, la trasmissione e la ricezione della posta elettronica. Per prima cosa dividerei gli apparati, di cui ci si serve per inviare in rete un messaggio di posta elettronica, in due categorie:

1. Sistemi hardware di cui si ha il possesso fisico (proprietà);
2. Sistemi di cui si è temporaneamente in possesso.

I primi a loro volta sono suddivisi in due categorie:

1. apparati fissi;
2. apparati mobili.

Gli apparati fissi sono ad esempio il PC che si ha in casa o nel proprio ufficio - specifico “proprio”, perché è ben diverso dal PC che si usa in un ufficio dove si ricopre comunque il ruolo di dipendenti, qualsiasi grado si abbia nella gerarchia - che invece va classificato nella seconda categoria (sistemi di cui si è temporaneamente in possesso). La proprietà dell’apparato è quella che si identifica molto spesso con colui che trasmette i messaggi di posta elettronica con quel dispositivo specifico, conseguentemente una prima importante ulteriore ripartizione è che: l’apparato può essere a disposizione di altri o può essere comunque usato da altri. Vedrete come ai fini della privacy e della sicurezza questa non sia una cosa banale, bensì estremamente importante. Stante lo sviluppo molto forte degli apparati mobili, va fatto su questi un approfondimento particolare. Essendo questi apparati “mobili”, hanno maggiori potenziali minacce come: la perdita o il furto di PC portatile o di un palmare, costituiscono un trauma non da poco nella vita personale e professionale di un individuo, con conseguenze a volte catastrofiche. La prudenza e la sicurezza per tutto quello che appartiene alla nostra sfera personale e professionale non sono mai troppe e non bisogna mai abbassare la guardia.
La sicurezza va affrontata con semplicità e naturalezza, quello che è complicato diventa tedioso ed alla fine non viene più usato, sia se dobbiamo regolare la materia con noi stessi, che nell’impartire disposizioni ad altri.
Complicazioni e complessità non implicano il concetto di sicurezza, mentre invece semplicità e naturalezza si tramutano spesso in operazioni abituali che facilitano la protezione dei sistemi usati.
La creazione di riflessi condizionati automatici sono il “goal” a cui si deve arrivare, cioè quella cosa che diventa naturale fare. Per esempio, in alcune zone in Italia si lascia ancora la chiave nella porta di casa mentre in altre si chiude a volte con complicatissime serrature doppie ed anche quadruple, s’innesta il sistema d’allarme e poi si esce.
Se si prova ad invertire i soggetti e colui che abita in zona tranquilla va abitare nell’altra, si vedrà che i comportamenti saranno diversi: il primo non riuscirà a compiere i dieci, venti gesti che l’altro compie tutti i giorni e dimenticherà l’una o l’altra cosa, il secondo si sentirà insicuro e non dormirà la notte. Qui di seguito alcuni semplici ac-

corgimenti da seguire. Non è ovviamente compito di questo libro suggerire questo o quel sistema di sicurezza o quella o altra password, temi che di per sé richiederebbero una pubblicazione a parte, ma solo abituare il lettore ad attuare minime azioni indispensabili per non correre rischi evitabili.

Apparati Fissi

La prima cosa è quella di mettere in sicurezza il "portone" d'accesso alla casa per poi via, via arrivare a proteggere la propria stanza, il cassetto della scrivania e via dicendo. Innanzitutto ed in particolar modo, se l'apparato è accessibile a molti soggetti, assicurare il sistema con idonea password: ogni PC è dotato di BIOS che ha diversi sistemi di sicurezza. Il BIOS nel PC non dipende da nessun software che si carichi nello stesso, è solo legato all'hardware della macchina, che come si accende, vi invita ad entrare nello stesso per alcuni impostazioni particolari.
Normalmente presenta un menù a tendina tipo Windows: cercate l'area marcata con sicurezza (security) ed inserite la vostra password che va assolutamente protetta scrivendola e conservandola in luogo sicuro. Difatti qualora persa, solo un intervento hardware sul PC potrà farlo funzionare.
Da quel momento in poi la macchina sarà accessibile solo a chi sarà in possesso della password, sebbene possono essere inseriti per l'accesso al sistema operativo anche successivi livelli di password con la complicazione di dover ricordare password multiple, oltre a tutte quelle che dobbiamo ricordare.
Va da sé che il livello di sicurezza è decisamente diverso in base all'uso che si fa del PC e si ritiene che difenderne l'accesso con il sistema di password del BIOS sia di per se stesso un sistema semplice e di media sicurezza che previene l'accesso all'intero PC, quindi anche a tutti i dati nello stesso conservati.

Apparati Mobili

La difesa dell'apparato mobile è assimilabile al fisso per quanto attiene a PC portatili, netbook e similari con una sola eccezione: in questo caso la difesa attraverso password del BIOS è meno efficace per il semplice fatto che il rischio del portatile è la perdita e/o furto. A quel punto chi ne entra in possesso ha tutto il tempo di fare tutti gli interventi utili per penetrare nel sistema. Vediamo quindi quale è

la parte da andare a proteggere, ovviamente con la speranza che o-gnuno abbia provveduto ad effettuare un backup dei dati contenuti nel proprio portatile; direi che la parte sensibile è l'hard disk. Bloccare l'accesso allo stesso con una password è una tecnica banale, ma può avere una certa efficacia sebbene sia il livello di segretezza e l'importanza che hanno i dati conservati che debbono influire sulla scelta del livello di protezione.
Si può arrivare a criptare l'intero contenuto dell'hard disk dato che in commercio c'è un numero sempre crescente di software che serve allo scopo.

CAPITOLO III. 3.0
POSTA ELETTRONICA E TRASMISSIONE SICURA DEI DOCUMENTI

Che la trasmissione attraverso Internet, di qualsiasi cosa, debba essere sicura, è un concetto che tutti dovrebbero avere appreso - anche a proprie spese - eppure non è così: in particolare per la posta elettronica, utilizzata in tutto il mondo per inviare e ricevere milioni di messaggi, molti di noi non proteggono le proprie comunicazioni e si comportano come una volta veniva fatto per le cartoline postali,

con l'aggravante che, contrariamente al sistema postale dove l'accesso fisico alle cartoline è limitato alle poche persone della "filiera" del sistema poste (portalettere, impiegati, addetti ecc.), coloro che possono accedere ai messaggi di posta elettronica e loro allegati sono oltre un miliardo di persone sparsi in tutto il mondo.

La compilazione di un form on-line in chiaro, cioè in una pagina Internet non protetta, è il modo per far vedere i propri dati ad un numero potenzialmente illimitato di utenti Internet e può costituire un pericolo ancora maggiore.

Come questo esempio

Il messaggio ed anche gli allegati possono essere intercettati e letti da chiunque. Un form on-line non protetto e' come l'orso ed il miele (dove l'hacker è l'orso ed il miele i dati inseriti).

La differenza peggiorativa e' che chi cerca di intercettare l'e-mail ha interesse a farlo, in entrambi i casi gli interessi sono numerosi.

Alcuni dei più significativi sono:

- Acquisizione e vendita di indirizzi e-mail, per successive operazioni di spamming;
- Acquisizione indirizzi e-mail riconducibili a Banche, per successive operazioni di phishing;
- Spionaggio industriale o di altro genere;
- Falsificazione e/o alterazione dei dati;

- Uso del proprio indirizzo e-mail e/o dei propri dati personali per scopi delittuosi;
- Vendita dei dati a terzi, ad esempio per campagne di marketing telefoniche sul fisso e/o sul cellulare;
- Studio delle abitudini/attitudini/preferenze delle persone;
- Intercettazioni di vario genere, che sembra, siano molto comuni oggi.

Pensare che sia una questione solo personale è un errore, mentre è facilissimo tracciare le e-mail e i loro destinatari.
Andando su Google e digitando *"e-mail is like postcard" o "tracking e-mail"* ci si rende conto quanto sia scritto a questo proposito.

Da molti anni si studia la soluzione per queste problematiche con modesti risultati.

<u>Quali requisiti deve avere un messaggio per essere sicuro?</u>

- **Certezza dell'autenticità del mittente;**
- **Integrità e non modificabilità dei dati ;**
- **Certezza dell'integrità del messaggio;**
- **Data e ora di spedizione e ricezione;**
- **Prova dell'avvenuta ricezione;**
- **Prova dell'apertura e lettura del messaggio e suoi allegati;**
- **Privacy;**
- **Non ripudio;**
- **Interoperabilità, conservando tutte le caratteristiche e gli standard di sicurezza in tutto il mondo.**

Più avanti si vedrà come questi principi di base abbiano influito sulla ricerca di una soluzione al problema attraverso la crittografia, la firma digitale e l'uso di appositi protocolli di trasmissione dei messaggi.

Vedremo anche come si è ancora lontani dall'aver risolto queste problematiche, in special modo quella che viene definita ***identità digitale.***

EVOLUZIONE DELLA SICUREZZA NELLA TRASMISSIONE DEI MESSAGGI: LA CRITTOGRAFIA, GLI ALGORITMI

L'uso sempre più massivo della posta elettronica iniziò ad avere delle serie problematiche in merito alla sicurezza e alla privacy dei messaggi spronando la ricerca al fine d'individuare sistemi sicuri per la trasmissione della stessa, da subito si capi che la crittografia era l'unico sistema per la soluzione del problema.

BREVE STORIA ED ANALISI DELLA CRITTOGRAFIA APPLICATA

I Message Digest sono una serie di algoritmi progettati dal prof. Ronald Rivest del MIT.

- Nel 1991, quando Had Dobbertin provò la debolezza dell'MD4, fu progettato da Ronal Rivest (nella foto) l'MD5, che rimpiazzò il suo predecessore MD4.

- Nel 1993 Der Boer e Bosselaers ottennero un primo risultato trovando una pseudo collisione dell'algoritmo MD5: cioè due diversi vettori di inizializzazione "i" e "j" con 4 bit di differenza tali che:
  MD5 compress(i,x) = MD5 compress (j,x)

- Nel 1996 Dobbertin rilevò una collisione nella funzione di MD5, ma anche se non presentava una problematica alla funzione hash MD5 completa, per molti crittografi fu sufficiente per andarlo subito a sostituire con il WHIRLPOOL, SHA1 o RIPEMD160.
  La cui dimensione dell'hash di 128 bit era abbastanza piccola per eseguire un *Birthday attack*.[24]

[24] *Wikipedia:* **attacco del compleanno** è un tipo di attacco crittografico utilizzato per la crittanalisi degli algoritmi di cifratura; è così chiamato perché sfrutta i princìpi matematici del paradosso del compleanno nella teoria delle probabilità.

- Nel marzo 2004 iniziò il progetto distribuito da MD5CRK, con lo scopo di dimostrare che l'MD5 era un algoritmo insicuro, trovando una collisione nell'usare un *birthday attack*.

Ronald Linn Rivest

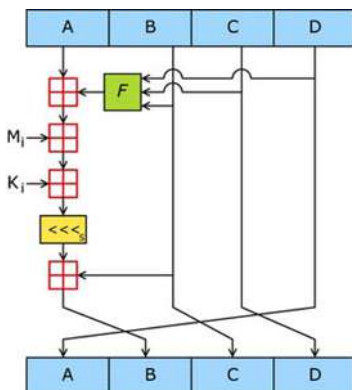
- Nell'agosto 2004 ebbe fine l'MD5CRK, quando fu trovata una collisione annunciata da Xiaoyun Wang.
- Nel marzo 2005 Arjen Lenstra, Xiaoyun Wang e Benne de Weger, dimostrarono la possibilità di costruire due certificati X509 con differenti chiavi pubbliche e lo stesso MD5 hash, dimostrando una collisione dell'algoritmo.

L'ALGORITMO MD5

L'MD5 (acronimo di Message Digest Algorithm) è un algoritmo per la crittografia dei dati a senso unico realizzato da Ronald Rivest[25] nel 1991 e standardizzato con RFC 1321.
Questo tipo di codifica prende in input una stringa di lunghezza arbitraria producendone un'altra a 128 bit (con lunghezza fissa di 32 valori esadecimali, indipendentemente dalla stringa di input), che può essere usata per calcolare la firma digitale dell'input.

---

[25] **Ronald Linn Rivest** (Schennectady, 1947) è un crittografo statunitense. Il suo lavoro più noto è sicuramente il sistema di crittografia asimmetrica che ha sviluppato assieme a Leonard Adleman e Adi Shamir: il crittosistema RSA (1978). Ha conseguito una laurea in Matematica presso l'Università Yale nel 1969 ed un dottorato di ricerca in Informatica presso l'Università di Stanford nel 1974. Attualmente è Professore di "Electrical Engineering and Computer Science" presso il Department of Electrical Engineering and Computer Science del MIT, dove guida il gruppo di Crittografia e Sicurezza delle Informazioni. Oltre ad essere coautore del crittosistema RSA è noto anche per aver progettato molti protocolli e algoritmi che sono stati spesso accettati come standard, come ad esempio i cifrari RC4 e RC5 e i sistemi di hash crittografico MD4 e MD5; ha collaborato anche ai lavori sul candidato AES RC6. La sua attività non si è limitata all'ambito accademico: ha avuto un ruolo significativo nel dibattito politico-sociale in corso fra le opposte esigenze del diritto alla tutela dei dati personali (privacy) da parte del cittadino e l'esigenza del controllo della sicurezza da parte dello stato. Attualmente si sta occupando della possibilità di realizzazione di sistemi elettronici per il voto elettronico che garantiscano l'anonimato del voto stesso.
È stato fondatore della società RSA Data Security (dopo la fusione con Security Dynamics la società è stata rinominata RSA Security) azienda leader nel settore della progettazione e vendita di applicazioni crittografiche. "Costola" poi della Verisign di cui Massimo Penco è stato direttore per l'Europa fino al 2001, azienda che ha spinto l'uso dell'SSL in tutto il mondo.
È stato Direttore dell'"International Association for Cryptologic Research" e della "Financial Cryptography Association". È membro dell'"American Academy of Arts and Sciences", dell' "Association for Computing Machinery" e della "National Academy of Engineering". Con Adi Shamir e Leonard Adleman, ha ricevuto il "2000 IEEE Koji Kobayashi Computers and Communications Award" e il "Secure Computing Lifetime Achievement Award".

La codifica avviene velocemente e si presuppone che l'output restituito sia univoco, che non ci siano possibilità, se non per tentativi, di risalire alla stringa di input (formata da due diverse stringhe) partendo dalla stringa di output (i cui possibili valori sono pari a 16 alla 32esima potenza), la stringa di output è nota come MD5 Checksum o MD5 Hash. La dimensione dell'hash di 128 bit, era abbastanza piccola per eseguire un *Birthday attack*[26].

- Nel 18 marzo 2006 Vlastimil Klima pubblicò un algoritmo che riusciva a trovare una collisione in un minuto su un singolo computer, usando un metodo che chiamò *"calls tunneling"*.

Applicazione dell'MD5

La crittografia, tramite l'algoritmo MD5, viene applicata in tutti i settori dell'informatica che lavorano con il supporto delle firme digitali, o che comunque trattano dati sensibili.
Ad esempio, viene utilizzata per controllare che uno scambio di dati sia avvenuto senza perdite od intrusione negli stessi, semplicemente con il confronto tra la stringa prodotta dal file inviato e la stringa prodotta dal file ricevuto. Con lo stesso metodo si può anche verificare se il contenuto del file è cambiato, diffuso anche come supporto per l'autenticazione degli utenti attraverso i linguaggi di scripting web server side.
Durante la registrazione di un utente su un portale Internet, la password scelta durante il processo verrà codificata tramite MD5 e

[26] *Wikipedia:* **attacco del compleanno** è un tipo di attacco crittografico utilizzato per la crittanalisi degli algoritmi di cifratura; è così chiamato perché sfrutta i principi matematici del paradosso del compleanno nella teoria delle probabilità.

la sua firma digitale verrà memorizzata nel database. Successivamente nel corso dell'operazione di login, la password immessa dall'utente, subirà lo stesso trattamento descritto precedentemente e verrà confrontata con la copia in possesso del server, per avere la certezza dell'autenticità. Nel testo che segue verrà illustrato il funzionamento del protocollo MD5.

DA SMTP E MIME A S/MIME E RELATIVA EVOLUZIONE

Dopo SMTP (Simple Mail Transfer Protocol[27]) e la sua evoluzione MIME, il protocollo per la posta elettronica accettato come standard a livello globale, che tuttavia presentava un limite intrinseco dal punto di vista della sicurezza, necessità non più procrastinabile, le implementazioni successive ebbero un forte dilemma da risolvere sicurezza o connettività. Non potendo includere entrambe le caratteristiche nel SMTP, venne introdotto un nuovo protocollo: S/MIME.

Con l'introduzione di S/MIME, si è potuta adottare una soluzione di posta elettronica, protetta a livello globale interoperabile in tutto il mondo. Caratterizzato da un livello di diffusione paragonabile a SMTP, lo standard S/MIME presenta funzionalità più avanzate rispetto al protocollo precedente, poiché consente un'ampia interoperabilità per la posta elettronica con il vantaggio della sicurezza.

Per comprendere meglio lo standard S/MIME (Secure Multipurpose Internet Mail Extensions) è utile conoscere la sua evoluzione.

[27] **Simple Mail Transfer Protocol** (**SMTP**) è il protocollo standard per la trasmissione via internet di e-mail. In italiano si potrebbe tradurre come "Protocollo elementare di trasferimento postale".
È un protocollo relativamente semplice, testuale, nel quale vengono specificati uno o più destinatari di un messaggio. Verificata la loro esistenza, il messaggio viene trasferito. È abbastanza facile verificare come funziona un server SMTP mediante un client telnet. Il protocollo SMTP utilizza come protocollo di livello transport TCP. Il client apre una sessione TCP verso il server sulla porta 25. Per associare il server SMTP a un dato nome di dominio (DNS) si usa un Resource Record di tipo MX (Mail eXchange) (Tipi di record DNS). SMTP iniziò a diffondersi nei primi anni '80. A quel tempo era un'alternativa a UUCP, che era più adatto a gestire il trasferimento di e-mail fra computer la cui connessione era intermittente. L'SMTP, d'altra parte, funziona meglio se i computer sono sempre collegati alla rete. Poiché SMTP è un protocollo testuale basato sulla codifica ASCII (in particolare ASCII NVT), non è permesso trasmettere direttamente un testo composto con un diverso set di caratteri e tantomeno file binari. Lo standard MIME permette di estendere il formato dei messaggi mantenendo la compatibilità col software esistente. Per esempio, al giorno d'oggi molti server SMTP supportano l'estensione 8BITMIME, la quale permette un trasferimento di un testo che contiene caratteri accentati (non-ASCII) senza bisogno di trascodificarlo. Altri limiti di SMTP, quale la lunghezza massima di una riga, impediscono la spedizione di file binari senza trascodifica. (Nota che per i file binari inviati con HTTP si utilizza il formato MIME senza bisogno di una trascodifica.) SMTP è un protocollo che permette soltanto di inviare messaggi di posta, ma non di richiederli ad un server. Per fare questo il client di posta deve usare altri protocolli, quali il POP3 (Post Office Protocol) e l'IMAP (Internet Message Access Protocol).

La prima versione di S/MIME viene sviluppata nel 1995 da un gruppo di fornitori di soluzioni di sicurezza. Inizialmente si trattava di una delle tante specifiche per la protezione dei messaggi, al pari di PGP *(Pretty Good Privacy[28])*.
Ai tempi della prima versione di S/MIME non esisteva un unico standard riconosciuto per i messaggi protetti, ma più standard concorrenti. Nel 1998 con la seconda versione di S/MIME, la situazione iniziò a cambiare. Infatti questa versione fu sottoposta allo *IETF (Internet Engineering Task Force)* per l'accettazione come standard Internet. In questo modo, S/MIME, divenne lo standard per la trasmissione e la sicurezza dei messaggi; un solo protocollo che raggruppa le funzioni di tutti gli altri.

La prima versione di S/MIME utilizzava due specifiche RFC di IETF:

- l'RFC 2311 che stabiliva lo standard per i messaggi;
- l'RFC 2312 che stabiliva lo standard per la gestione dei certificati digitali che accompagnano i messaggi di posta elettronica.

Queste due specifiche RFC costituivano il primo framework basato su standard Internet disponibile per la realizzazione di soluzioni integrate per la protezione di messaggi. Nel 1999, per potenziare le funzionalità di S/MIME, l'ente IETF propose l'introduzione della terza versione di S/MIME, che comprende le seguenti specifiche: l'RFC 2632, che si basa sull'RFC 2311 per definire ulteriori standard per i messaggi S/MIME; l'RFC 2633, che potenzia la specifica RFC 2312 per la gestione dei certificati; l'RFC 2634, che estende le funzionalità dello standard S/MIME mediante la funzione di servizi aggiuntivi quali le conferme e le etichette di protezione, nonché la tripla crittografia.
Con la terza versione il protocollo S/MIME ha ottenuto un riconoscimento a livello mondiale come standard nella protezione dei mes-

[28] **Pretty Good Privacy** (**PGP**) è un programma che permette di usare autenticazione e privacy crittografica. Nelle sue varie versioni è probabilmente il crittosistema più usato al mondo. In *Applied Cryptography*, il crittografo Bruce Schneier lo ha descritto come il modo per arrivare "probabilmente il più vicino alla crittografia di livello militare" PGP è stato originariamente sviluppato da Phil Zimmermann nel 1991. Il nome gli è stato suggerito da una drogheria di Lake Wobegon, l'immaginaria città natale dello speaker radio Garrison Keillor. La drogheria si chiamava "Ralph's Pretty Good Grocery" ("la drogheria piuttosto buona di Ralph") e il suo slogan era "se non lo puoi trovare da Ralph, probabilmente puoi anche farne a meno".

saggi ed è supportato fra l'altro dai seguenti software della Microsoft:

- Microsoft Outlook 2000 (con SR1) e versioni successive;
- Microsoft Outlook Express 5.01 e versioni successive;
- Microsoft Exchange 5.5 e versioni successive.

Ora, tutti gli altri principali sistemi client e web di posta elettronica si sono evoluti con l'uso di S/MIME come pure gli apparati mobili, particolare menzione va al Blackberry, che ha un'approfondita documentazione tecnica in merito, consultabile on-line, veramente esaustiva applicabile a qualsiasi altro apparato mobile[29].

SERVIZI OFFERTI DA S/MIME

S/MIME basa la sua architettura su un'infrastruttura a chiavi pubbliche *(PKI[30])* e fornisce due servizi di protezione:

- Firme digitali;
- Crittografia dei messaggi.

Questi due servizi sono alla base della protezione dei messaggi S/MIME. Ad essi sono correlati tutti gli altri concetti relativi alla protezione. Benché apparentemente complessa, la protezione dei messaggi è basata sulle firme digitali e sulla crittografia dei messaggi.

LE FIRME DIGITALI CON IL PROTOCOLLO S/MIME

Le firme digitali sono il servizio utilizzato da S/MIME. Come indicato dalla definizione, queste sono il corrispondente digitale delle firme tradizionali, con effetto legale, apposte ai documenti cartacei.

[29] http://docs.blackberry.com/en/smartphone_users/deliverables/20426/SMIMEprotected_messages_64974_11.jsp

[30] In crittografia un'**infrastruttura a chiave pubblica** in inglese **Public Key Infrastructure** (**PKI**) è una serie di accordi che consentono, a terze parti fidate, di verificare e/o farsi garanti dell'identità di un utente, oltre che di associare una chiave pubblica a un utente, normalmente per mezzo di software distribuito in modo coordinato su diversi sistemi. Le chiavi pubbliche tipicamente assumono la forma di certificati digitali. Il termine PKI viene usato per indicare sia l'autorità di certificazione e i relativi accordi, che, in senso più esteso, l'uso di algoritmi crittografici a chiave pubblica nelle comunicazioni elettroniche. L'uso del termine nell'ultimo senso è errato in quanto una PKI non necessariamente richiede l'uso di algoritmi a chiave pubblica. La struttura della PKI non solo riguarda la CA, ma anche la **Registration Authority**, attraverso la quale gli utenti si rivolgono per richiedere la certificazione delle chiavi, identificandosi e fornendo almeno la chiave pubblica e l'indirizzo e-mail. il **Certificate Server** ovvero un servizio di directory accessibile mediante un "operational protocol", tipicamente LDAP; che è principalmente una lista di pubblicazione dei certificati e delle liste dei certificati revocati e sospesi.

Analogamente a quelle tradizionali, le firme digitali presentano le seguenti caratteristiche di protezione:

Autenticazione e Validazione
Una firma ha la funzione di convalidare un'identità, consentendo ad ogni singola identità di distinguersi da tutte le altre e di provare la propria univocità. Nella posta elettronica basata su SMTP non è prevista l'autenticazione e non è possibile conoscere l'effettivo mittente di un messaggio. Per ovviare a questo problema è disponibile l'autenticazione tramite firma digitale, che consente al destinatario di un messaggio di verificare se quest'ultimo è stato effettivamente inviato dal presunto mittente.

"Non ripudio"
Il carattere di unicità di una firma impedisce al relativo proprietario di
disconoscerla. Questa caratteristica è definita "non ripudio". L'autenticazione tramite firma consente di avvalersi del "non ripudio". Questo concetto è particolarmente diffuso nell'ambito dei contratti scritti. Un contratto firmato è un documento legalmente vincolante ed è quindi impossibile disconoscere una firma autenticata da un notaio o da un pubblico ufficiale nella nostra legislazione, mentre nei paesi anglosassoni è invalso l'uso dei testimoni alla firma di un atto. Le firme digitali svolgono questa stessa funzione, e soprattutto in determinati settori, sono sempre più riconosciute come legalmente vincolanti, proprio come una firma autenticata su carta. Poiché la posta elettronica basata su SMTP non fornisce alcun mezzo di autenticazione, non è in grado di garantire il non ripudio. Qualsiasi mittente può disconoscere la proprietà di un messaggio di posta elettronica SMTP.

Integrità dei dati e non modificabilità dei dati
E' un servizio di protezione aggiuntivo risultante dalle operazioni che consentono l'utilizzo delle firme digitali . Con questo servizio, quando il destinatario di un messaggio di posta elettronica con firma digitale esegue la convalida della firma, ha la sicurezza che il messaggio ricevuto non sia stato modificato durante il trasferimento. Se dopo la firma il messaggio viene modificato, la firma non sarà più

valida ed esaminando l'header del messaggio si noterà subito la modifica.
I sistemi di posta elettronica in netta evoluzione sul lato sicurezza inviano un *alert,* qualora il messaggio sia stato modificato.
In questo modo, le firme digitali forniscono un tipo di garanzia che le firme su carta non sono in grado di offrire, poiché un documento cartaceo può essere modificato anche dopo la firma, normalmente apposta nell'ultima pagina, in una parte dello stesso.
Le firme digitali garantiscono l'integrità dei dati ma non la riservatezza. I messaggi con firma digitale vengono inviati come testo non crittografato analogamente ai messaggi SMTP, non possono essere modificati ma possono essere letti da altri utenti. I messaggi con firma crittografata sono caratterizzati da un determinato livello di protezione in quanto sono codificati in base allo standard base 64 pur non essendo inviati come testo non crittografato.
Per proteggere quindi il contenuto della posta elettronica è necessario utilizzare la crittografia. L'autenticazione, il "non ripudio" e l'autenticità dei dati sono le caratteristiche delle firme digitali. Queste tre funzioni garantiscono al destinatario di un messaggio che questo è stato inviato dal mittente specificato e che non è stato modificato durante la trasmissione.
L'utilizzo della firma digitale comporta l'applicazione della firma al testo del messaggio di posta elettronica al momento dell'invio e la verifica di tale firma alla lettura del messaggio ricevuto.

GESTIONE DELLA POSTA ELETTRONICA CON S/MIME

Una volta capito il sistema di funzionamento del protocollo S/Mime e delle sue funzioni vediamo la sua pratica applicazione, consiglio vivamente di installare uno dei certificati S/Mime gratuiti, facilmente reperibili nel web, sarà molto più semplice vedere nella pratica come funziona.

Applicazione di una firma digitale e verifica della firma in un messaggio di posta elettronica

Per firmare digitalmente un messaggio di posta elettronica sono richieste informazioni che possono essere fornite solo dal mittente. Durante l'operazione di firma le informazioni fornite dal mittente vengono utilizzate per l'acquisizione del messaggio di posta elettro-

nica e l'applicazione della firma digitale. Al termine dell'operazione viene generata la firma digitale effettiva, che viene quindi inclusa ed inserita nel messaggio al momento dell'invio.

Nella figura: firma digitale in un messaggio di posta elettronica

Le operazioni che vengono effettuate automaticamente sono:

1. Acquisizione del messaggio;
2. Recupero delle informazioni che identificano il mittente in maniera univoca;
3. Applicazione al messaggio di una firma digitale generata in base alle informazioni univoche del mittente;
4. Aggiunta della firma digitale al messaggio;
5. Invio del messaggio: poiché quest'operazione richiede l'inserimento di informazioni univoche da parte del mittente, le firme digitali forniscono sia l'autenticazione, che il "non ripudio". Queste informazioni provano che il messaggio può essere inviato solo dal mittente.

Però nessun meccanismo di protezione è perfetto. E' possibile che le informazioni univoche utilizzate dal mittente per l'applicazione delle firme digitali vengano acquisite da utenti non autorizzati, che possono così simulare l'identità del mittente.
Tuttavia lo standard S/MIME è in grado di gestire questa situazione mostrando come non valide le firme non autorizzate. Quando il messaggio di posta elettronica con firma digitale viene aperto dal destinatario, viene eseguita la procedura di verifica della firma.

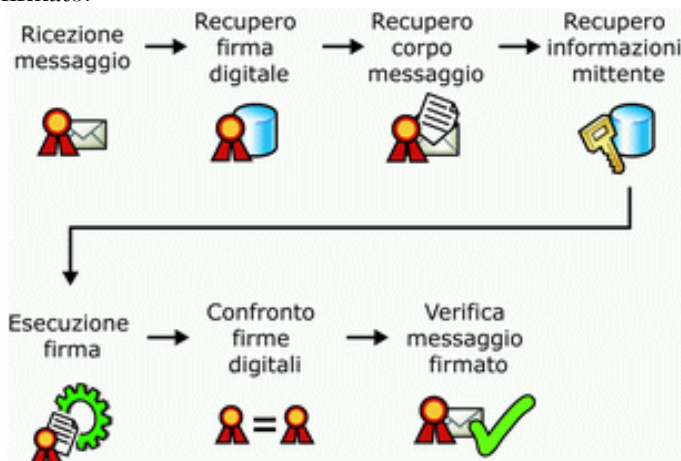
Questa procedura consiste nel recupero della firma digitale, del messaggio originale e nell'esecuzione di un'altra operazione di firma, con conseguente generazione di un'altra firma digitale. Le due firme

vengono poi confrontate. Se corrispondono si ha certezza che il messaggio proviene effettivamente dal mittente, altrimenti il messaggio viene contrassegnato come non valido.

Verifica di una firma digitale di un messaggio di posta elettronica:

1. Ricezione del messaggio;
2. Recupero della firma digitale del messaggio;
3. Recupero corpo del messaggio;
4. Recupero delle informazioni identificative del mittente;
5. Operazioni di firma nel messaggio;
6. Confronto della firma digitale inclusa nel messaggio con quella generata al momento della ricezione;
7. Verifica delle firme del messaggio. Se le firme corrispondono il messaggio è valido.

Le informazioni utilizzate dal destinatario sono correlate in modo da consentire a quest'ultimo di verificare l'autenticità delle informazioni univoche del mittente, senza effettivamente conoscere il contenuto, garantendone così la riservatezza.

Il processo di applicazione e verifica della firma digitale, consiste sostanzialmente nell'autenticare il mittente di un messaggio di posta elettronica e di determinare l'integrità dei dati all'interno del messaggio firmato.

Nella figura sopra viene indicato schematicamente il processo di verifica della firma digitale.

Se le informazioni del mittente utilizzate per la verifica della firma, non corrispondono a quelle fornite dal mittente al momento della firma del messaggio il sistema genererà un errore che avvertirà sia il mittente, che il destinatario dell'avvenuta alterazione del messaggio o suoi allegati. Le informazioni utilizzate dal destinatario sono correlate in modo da consentire a quest'ultimo di verificare l'autenticità delle informazioni univoche del mittente, senza aver bisogno di conoscere il contenuto del messaggio stesso, garantendone comunque la riservatezza.
Il processo di applicazione e verifica della firma digitale, consiste sostanzialmente nell'autenticare il mittente di un messaggio di posta elettronica e di determinare l'integrità dei dati all'interno del messaggio firmato.
L'autenticazione dei mittenti fornisce funzionalità aggiuntive di "non ripudio" che impediscono ai mittenti autenticati di disconoscere la proprietà di un messaggio inviato. Le firme digitali forniscono una soluzione ai problemi di identità e manomissione dei dati, che possono verificarsi con la posta elettronica Internet basata su SMTP.

Crittografia dei messaggi
La crittografia dei messaggi offre una soluzione per la riservatezza delle informazioni. I messaggi di posta elettronica Internet basati su SMTP, non sono protetti. Possono essere intercettati e letti, modificati, alterati, falsificati da qualsiasi utente durante la fase di trasmissione o nell'area stessa in cui vengono archiviati.
Questi problemi non si verificano se si utilizza lo standard S/MIME.
La crittografia fornisce il metodo per modificare le informazioni in modo da impedirne la lettura, uno dei punti più deboli della posta elettronica.
La crittografia dei messaggi fornisce due servizi di protezione specifici:
Riservatezza
La crittografia consente di proteggere il contenuto di un messaggio di posta elettronica, rendendolo accessibile solo al destinatario speci-

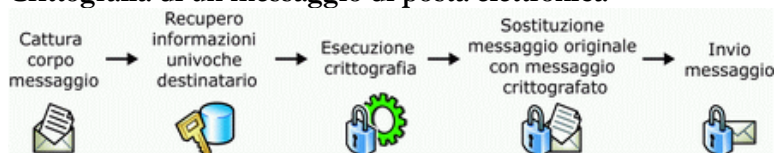
ficato. In questo modo viene garantita la massima riservatezza del messaggio durante il trasferimento o nell'area di archiviazione.

Integrità dei dati

Analogamente alle firme digitali, anche le operazioni di crittografia dei messaggi garantiscono l'integrità dei dati.
La crittografia dei messaggi garantisce invece la riservatezza dei dati ma non esegue l'autenticazione del mittente. Un messaggio crittografato senza firma digitale può essere soggetto a problemi di sostituzione di identità, come un messaggio non crittografato. Allo stesso modo la crittografia non garantisce il "non ripudio", poiché questa caratteristica è il risultato diretto dell'autenticazione.
Inoltre l'integrità dei dati di un messaggio crittografato è garantita solo dal momento dell'invio. Non sono quindi disponibili informazioni riguardanti il mittente del messaggio e per provare l'identità del mittente, il messaggio deve contenere la firma digitale.
La riservatezza e l'integrità dei dati costituiscono le caratteristiche principali della crittografia dei messaggi.
Queste due funzioni precisano infatti che solo il destinatario specificato sarà in grado di visualizzare il messaggio e che il messaggio ricevuto corrisponde esattamente a quello inviato. La crittografia ha lo scopo di rendere illeggibile e inalterabile il testo dei messaggi e i suoi allegati, prima che questi vengano inviati attraverso la rete. Al termine della ricezione il testo viene reso nuovamente leggibile tramite un'operazione di decrittografia.

Operazioni di crittografia e decrittografia di un messaggio di posta elettronica

L'operazione di crittografia eseguita al momento dell'invio, rende illeggibile il messaggio in quanto utilizza le informazioni relative al certificato del destinatario specificato. Il messaggio crittografato sostituisce quello originale e viene contemporaneamente inviato al destinatario.

Crittografia di un messaggio di posta elettronica

Per la crittografia di un messaggio di posta elettronica vengono compiute le seguenti operazioni in modo automatico:

1. Acquisizione del messaggio;
2. Recupero delle informazioni che identificano il messaggio in maniera univoca;
3. Crittografia del messaggio in base alle informazioni relative al destinatario;
4. Sostituzione del testo originale del messaggio con quello crittografato;
5. Invio del messaggio.

Richiedendo l'utilizzo di informazioni univoche relative al destinatario, la crittografia dei messaggi garantisce la riservatezza dei dati. Solo il destinatario specificato dispone delle informazioni necessarie per decrittografare il messaggio, e quindi solo questo utente è in grado di visualizzarlo.

Le informazioni del destinatario utilizzate per la crittografia del messaggio non corrispondono a quelle fornite dal destinatario per l'operazione di decrittografia. Le informazioni visualizzate dal mittente sono correlate in modo da consentire a quest'ultimo di verificare l'autenticità delle informazioni univoche del destinatario, senza effettivamente conoscere il contenuto, garantendone così la riservatezza.

Quando il destinatario apre un messaggio crittografato viene eseguita un'operazione di decrittografia: vengono recuperati sia il messaggio crittografato, che le informazioni univoche del destinatario da utilizzare per la decrittografia del messaggio.

Per effetto di quest'operazione, viene restituito il messaggio, viene decrittografato e risulta così visibile al destinatario.

Se il messaggio fosse stato modificato durante la trasmissione, l'operazione di crittografia non sarebbe riuscita.

Decrittografia di un messaggio di posta elettronica

Per la decrittografia di un messaggio di posta elettronica vengono compiute le seguenti operazioni in modo automatico:

1. Ricezione del messaggio;
2. Recupero del messaggio crittografato;
3. Recupero delle informazioni che identificano il destinatario in maniera univoca;
4. Decrittografia del messaggio crittografato in modo da generare un messaggio decrittografato in base alle informazioni univoche del destinatario;
5. Recapito del messaggio non crittografato al destinatario;

6. Il processo di crittografia e decrittografia garantisce la riservatezza dei messaggi e consente di risolvere uno dei problemi più critici della posta elettronica.

Ovviamente, tutte le operazioni anzidette valgono anche per gli allegati al messaggio di posta elettronica.
Il complesso della procedura di firma dei messaggi e dei suoi allegati viene realizzata attraverso il sistema definito *PKI (Pubblic Key Infrastructure)* Infrastruttura a Chiavi Pubbliche.

Interazione delle firme digitali con la crittografia dei messaggi
Le firme digitali e la crittografia dei messaggi non si escludono reciprocamente.

Ciascuno di questi servizi consente di risolvere problemi specifici di protezione del messaggio.
Le firme digitali forniscono il supporto per l'autenticazione e il "non ripudio", mentre la crittografia garantisce la riservatezza dei messaggi.
In considerazione dei diversi ruoli svolti, entrambi i servizi sono normalmente richiesti nell'ambito di una stessa strategia di protezione dei messaggi.

L'integrità di questi due servizi è importante poiché ciascuno si interessa di un diverso aspetto della relazione mittente-destinatario.

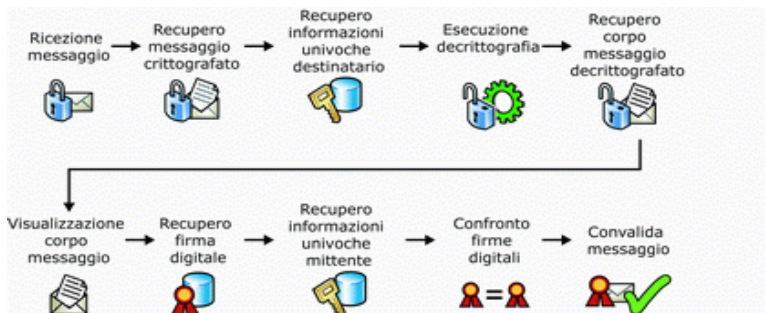
Le firme affrontano le problematiche relative ai mittenti, mentre la crittografia le problematiche relative ai destinatari. Entrambi garantiscono l'inviolabilità dei messaggi.

Quando le firme digitali e la crittografia dei messaggi vengono utilizzati insieme, gli utenti possono beneficiare di entrambi i servizi e la modalità di gestione e di elaborazione dei due servizi rimane invariata.

Funzionamento della firma digitale e crittografia di un messaggio di posta elettronica

Durante l'intera procedura di firma digitale e crittografia di un messaggio di posta elettronica vengono compiute le seguenti operazioni in modo automatico:

1. Acquisizione del messaggio;
2. Recupero delle informazioni che identificano il mittente in maniera univoca;
3. Recupero delle informazioni che identificano il destinatario in maniera univoca;
4. Applicazione al messaggio di una firma generata in base alle informazioni univoche del mittente;
5. Aggiunta della firma digitale al messaggio;
6. Crittografia del messaggio in base alle informazioni relative al destinatario;
7. Sostituzione del messaggio originario con quello crittografato;
8. Invio del messaggio.

Quanto segue descrive invece l'operazione inversa, la quale consiste nella decrittografia del messaggio di posta elettronica e verifica della firma digitale

Più analiticamente, la procedura di decrittografia di un messaggio di posta elettronica e la verifica della firma digitale consistono invece nelle seguenti operazioni che vengono effettuate automaticamente dal sistema:

1. Ricezione del messaggio;
2. Recupero del messaggio crittografato;
3. Recupero delle informazioni che identificano il destinatario in maniera univoca;
4. Decrittografia del messaggio decrittografato in modo da generare un messaggio non crittografato in base alle informazioni univoche del destinatario;
5. Restituzione del messaggio non crittografato;
6. Recapito del messaggio non crittografato al destinatario;
7. Recupero della firma digitale dal messaggio non crittografato;
8. Recupero delle informazioni identificative del mittente;
9. Applicazione al messaggio non crittografato di una firma generata in base alle informazioni del mittente;
10. Confronto della firma digitale inclusa nel messaggio con quella generata al momento della ricezione;
11. Se le firme corrispondono ed il sistema non evidenzia errori il messaggio è valido, altrimenti non potrà essere aperto.

Ecco qui di seguito uno dei classici errori di sistema:

Messaggi con tripla crittografia

Uno dei perfezionamenti apportati nella terza edizione dello standard S/MIME, è rappresentato dalla tripla crittografia.

Un messaggio S/MIME con tripla crittografia è un messaggio firmato, crittografato, quindi nuovamente firmato. Questo ulteriore livello di crittografia fornisce una protezione avanzata dei messaggi.

Le firme digitali e la crittografia dei messaggi sono due servizi complementari in grado di fornire una protezione completa ai problemi di protezione che interessano la posta elettronica Internet basata su SMTP.

Identità digitale

Malgrado tutte le accortezze sopra descritte, siano garanzia avanzata nella sicurezza delle e-mail, non riescono tuttavia ad assicurare in modo assoluto l'identità del mittente e del destinatario, rimanendo un problema insoluto, a meno che non si è in possesso di sistemi avanzati e costosi, come apparati biometrici od altro. Vista la rilevanza delle problematiche connesse con l'uso delle e-mail ed altri apparati di comunicazione ho ampliato alcuni concetti come segue:

CAPITOLO IV. 4.0

BEST PRACTICE SULL'USO DELLA POSTA ELETTRONICA

Questa parte dovrebbe costituire un manuale a se stante ad uso di un singolo utente o di un'azienda per l'uso comune della posta elettronica.
La Posta Elettronica Certificata e la firma digitale sono ormai una realtà consolidata in tutto il mondo. I produttori di software/hardware sono sempre più attenti a questo fenomeno, che fra l'altro, si avvicina e si integra sempre più con la messaggistica dei cellulari con il recente annuncio di Microsoft, si immagina quindi che in futuro tutti i cellulari avranno a bordo il proprio sistema operativo, probabilmente Windows Mobile, già abbastanza diffuso.
Come ogni strumento, è soggetto a svariate problematiche e critiche, ma in finale è anche il mezzo più rapido ed economico che è stato mai inventato per trasmettere dati e come ogni strumento va usato con la dovuta attenzione.
Ho pensato sia utile scrivere alcune chiare e semplici regole per utilizzare le e-mail e la firma digitale in modo più sicuro, rapido ed efficiente. Questa **Best Practice** è indirizzata alle aziende, istituzioni, ma può essere anche una buona norma nell'uso privato.

La situazione ed alcuni dati salienti

La gestione della posta elettronica costituisce una seria questione per tutte le aziende ed istituzioni:

- E' protagonista ormai dal 25% al 50% delle attività quotidiane (fonte AIIM)
- Custodisce fino al 75% delle conoscenze aziendali e dati sensibili (Fonte Gartner)
- Oltre 171 miliardi di messaggi transitano ogni giorno nella rete Internet (Fonte AIIM 2006)
- Purtroppo il 70% di essi sono spamming (Fonte AIIM 2006)
- L'e-mail è sempre più usata come prova durante procedure legali

- La firma digitale è una componente inscindibile dell'e-mail come mezzo di trasmissione di documenti ed ora anche per le Fatture Elettroniche, E-Invoice[31] un importante progetto Europeo.

Eppure
Malgrado tutto questo, pochissime organizzazioni hanno intrapreso un progetto di gestione organica della corrispondenza elettronica e del suo uso sicuro.

Le ragioni della diffusione delle e-mail
Oggi le e-mail assolvono a tre diverse fondamentali funzioni, le quali possono essere elencate come segue:

1. Mezzo di comunicazione rapido ed economico;
2. Strumento semplice ma immediato di archiviazione;
3. Efficace ausilio nella collaborazione interna ad un'organizzazione;
4. Sistema unico per l'invio di documenti anche fiscali (fatture).

SCELTA DEL SISTEMA DI POSTA ELETTRONICA E DEL PROVIDER

Ci sono due sistemi per inviare e ricevere posta che possono essere integrati fra loro od usati entrambi: web-mail e client-mail.

WEB-MAIL[32]: E' il sistema in cui per leggere, inviare o ricevere e-mail ci si collega tramite Internet ad un server di posta elettronica. Ad esempio *g-mail* di Google uno dei tanti sistemi di posta elettronica gratuita. Forse è uno dei sistemi più usati. E' bene esaminarne i

[31] La fattura elettronica, intesa come l'anello di congiunzione tra i processi amministrativi ed i processi finanziari, rappresenta infatti un importante punto di snodo per procedere verso una più completa **integrazione dell'intero ciclo ordine-consegna-fatturazione- pagamento**, all'interno delle organizzazioni e soprattutto nelle relazioni di filiera con clienti e fornitori.
I servizi offerti dai consorziati attraverso il CBI permettono ad esempio ad un'azienda, che genera una fattura da un ordine, di richiederne anche il relativo pagamento inserendo alcuni dati che consentono, a pagamento ricevuto, di riconciliare la fattura con i fondi in entrata. http://ec.europa.eu/enterprise/sectors/ict/e-invoicing/benefits/index_en.htm

[32] Una ***Webmaill*** è un'applicazione *web* che permette di gestire uno o più *account* di posta elettronica attraverso un navigatore *web*. Generalmente viene fornita come servizio ad abbonati di un *provider* di connessione *internet*, oppure come servizio gratuito di posta elettronica. In alcune aziende la *webmail* viene fornita come servizio ai dipendenti, in modo che possano leggere la propria posta da casa oppure fuori sede. Attraverso l'interfaccia grafica si stabilisce una normale connessione verso un server di posta SMTP, IMAP o POP (POP3). Generalmente si utilizza IMAP per la sua struttura a cartelle sottoscrivibili.

pregi e i difetti che sono più o meno evidenti in base all'uso che si deve fare e all'affidabilità del provider.

VANTAGGI:
1) Si può usare da qualsiasi postazione e non si ha bisogno del proprio PC;
2) Gli archivi della propria posta elettronica sono conservati dal provider del servizio.

SVANTAGGI:
1) I dati sono conservati da una terza parte fino alla loro cancellazione, non è consigliabile lasciare la propria corrispondenza solo nel server del provider.

CLIENT-MAIL: E' il sistema in cui, pur dovendo sempre usufruire di un provider, si decide di usare uno dei sistemi di posta elettronica nel proprio PC (es. Outlook di Microsoft, Thunderbird od altri). Normalmente, tutto il traffico di posta elettronica deve essere gestito dal proprio PC, conservando il più delle volte la possibilità di lavorare con la propria casella di posta anche andando direttamente nel server del provider operando come descritto nel punto precedente. In appendice si potranno trovare le configurazioni dei maggiori provider di posta elettronica per la creazione di un account client nel proprio PC.
Molto spesso la complessità consiste nell'installare nel proprio PC il relativo account di posta elettronica, gestito con un sistema WEB, per la difficoltà a reperire i due elementi fondamentali per l'istallazione POP3[33] e SMTP. In appendice si troverà la lista dei più comuni.

VANTAGGI:
1) Massima flessibilità e possibilità di usare entrambi i sistemi;

[33] Il **Post Office Protocol** (detto anche **POP**) è un protocollo che ha il compito di permettere, mediante autenticazione, l'accesso ad un account di posta elettronica presente su di un host per scaricare le e-mail del relativo account. Il pop (nella versione 3) rimane in attesa sulla porta 110 dell'host (di default, ma può anche essere diversa) per una connessione TCP da parte di un client. I messaggi di posta elettronica, per essere letti, devono essere scaricati sul computer (questa è una notevole differenza rispetto all'IMAP), anche se è possibile lasciarne una copia sull'host. Il protocollo POP3 non prevede alcun tipo di cifratura, quindi le password utilizzate per l'autenticazione fra server e client passano **in chiaro**. Per risolvere questo possibile problema è stata sviluppata l'estensione **APOP** che utilizza MD5.

2) Gli archivi della propria posta elettronica possono essere lasciati sia nel server del provider, per un tempo che si potrà decidere, sia nel proprio PC.

SVANTAGGI:
Se si vuole gestire la posta elettronica solo dal proprio PC si ha bisogno della disponibilità fisica dello stesso.

Scelta del Provider
E' un aspetto molto importante da considerare per una molteplicità di motivi:

1) Affidabilità e fruibilità, sono i principali requisiti;
2) Spazio a disposizione nel server del provider. È indispensabile in special modo se si usa solo web-mail, ma è altresì importante per coloro che non accedono in modo continuo alla propria casella di posta. La possibilità che la stessa venga intasata e resa quindi non disponibile, non dipende dall'utente ma da coloro che gli inviano i messaggi;
3) Sistemi di sicurezza con un buon antivirus che protegga ciò che arriva nella casella di posta elettronica ed un ottimo antispamming. Il rischio di veder respingere per motivi futili, come gli allegati di grandi dimensioni, può impedire l'arrivo di documenti importanti;
4) La possibilità di usufruire di sistemi di sicurezza nei messaggi come ad esempio il protocollo S/MIME che vi permetterà di firmare e criptare il messaggio con i relativi allegati;
5) Affidabilità di assistenza e possibilità di usare web-mail con un client. Gmail, ad esempio, fornisce nel link del supporto un servizio ottimo e completo, in lingua italiana:
http://mail.google.com/support/

Elenco dei client POP supportati
Una volta attivata la funzione POP in Gmail, puoi configurare il tuo client di posta elettronica o dispositivo wireless per poter scaricare i messaggi Gmail. Per conoscere le impostazioni consigliate o risolvere i problemi POP, fai clic sul nome del tuo client di posta elettronica o dispositivo wireless nell'elenco riportato qui in basso. Se il tuo client di posta elettronica non è incluso in

questo elenco, siamo spiacenti, ma non siamo in grado di fornire assistenza per la configurazione.

Client di posta elettronica
Apple Mail 3.0[34]
Outlook Express[35]
Outlook 2002[36]
Outlook 2003[37] (visualizza la nostra demo animata)[38]
Outlook 2007[39]
Thunderbird 2.0[40]
Windows Mail[41]
Altro[42]

Dispositivi wireless
BlackBerry® Internet Service[43]
iPhone[44]

Telefoni cellulari
Per istruzioni su come accedere a Gmail per cellulari, visita la pagina dell'argomento Accesso tramite cellulare[45]

COME DEVE ESSERE UN'E-MAIL PROFESSIONALE E SOPRATTUTTO SICURA?

Scegliere il **FORMATO** in base al tipo dei messaggi aziendali che normalmente si inviano:

- **HTML:** è il formato con la veste grafica più bella, non accettato da tutti, ma sicuramente quello che colpisce di più;
- **TESTO:** solo testo privo di grafica ed immagini;

[34] http://mail.google.com/support/bin/answer.py?answer=13275
[35] http://mail.google.com/support/bin/answer.py?answer=13276
[36] http://mail.google.com/support/bin/answer.py?answer=70770
[37] http://mail.google.com/support/bin/answer.py?answer=13278
[38] http://mail.google.com/mail/help/demos/Gmail_POP/788_Google_Gmail.html
[39] http://mail.google.com/support/bin/answer.py?answer=86373
[40] http://mail.google.com/support/bin/answer.py?answer=38343
[41] http://mail.google.com/support/bin/answer.py?answer=86382
[42] http://mail.google.com/support/bin/answer.py?answer=13287
[43] http://mail.google.com/support/bin/answer.py?answer=14748
[44] http://mail.google.com/support/bin/answer.py?answer=72454
[45] http://www.google.com/support/mobile/?hl=it

- **RTF:** un compromesso tra i due precedenti;
- **CARATTERE:** può sembrare banale, ma la scelta del carattere ha un impatto molto importante per chi riceve un'e-mail ed inoltre è un sistema per "mitigare" tutti i rischi connessi.

Evitare caratteri strani, scegliere un carattere che tutti hanno normalmente installato nel proprio PC, perché inviare messaggi con caratteri non riconoscibili può invalidare il contenuto degli stessi. Invitare tutti, con una comunicazione di servizio, ad usare lo stesso carattere, con lo stesso corpo. Infatti, se qualcuno riceverà un'e-mail con carattere diverso, avrà quantomeno il sospetto che non venga dalla stessa persona o dalla stessa azienda.

Mittente: è importante non solo ai fini della sicurezza, ma anche ai fini della "netiquette"[46], che venga indicato in chiaro il nome e il cognome del mittente. Evitare anche di inserire appellativi generici come Avv., Studio, Dott., Soc., che non si riferiscono alla persona od ente e fanno letteralmente impazzire chi li deve gestire nella rubrica alfabetica: il titolo infatti apparirà per primo nell'ordine alfabetico.

Indirizzi di Posta Elettronica: vanno oculatamente scelti e resi standardizzati. Se l'azienda vuole attuare una politica di riservatezza dei propri dipendenti, gli indirizzi e-mail non dovranno essere semplici da trovare. Gli indirizzi e-mail come nome.cognome@sito.it sono facilmente rintracciabili e più inclini alla ricezione di messaggi indesiderati. E' opportuno usare il sistema di anagrammare le parole inserendo prima il cognome e poi alcune lettere del nome: pencoma@globaltrust.it e vedrete che lo spamming ecc. diminuiranno sensibilmente.

Firma: come la vecchia corrispondenza le e-mail vanno firmate da chi le spedisce. In questo modo viene rispettata la "netiquette" ed inoltre non costa nulla. Basta impostarla nel proprio programma di posta elettronica e verrà inserita automaticamente ogni qualvolta si crea, si risponde o si inoltra un messaggio in base alla regola fissata.

[46] http://www.nic.it/NA/netiquette.txt

Anche molti software di web mail danno la possibilità di inserire una propria firma .

Grafica della Firma: in base alla scelta del **FORMATO** potrete decidere come crearla.

DISCLAIMER: è essenziale inserire sempre un **disclaimer** per la posta elettronica che si invia. Qualora si usi un certificato di firma (altamente raccomandato) è bene inserire il **disclaimer** nel corpo dell'e-mail possibilmente sotto la firma con un carattere piccolo.

Alcuni esempi di disclaimer generici:

1. DISCLAIMER

This message and any information contained within it, including but not limited to subject matter, addressees and their e-mail addresses and attachments hereto are intended only for the personal and confidential use of the designated recipients named herein. Internet communications may not be secure and may be intercepted, redirected or spoofed and therefore XXXXXX does not accept legal responsibility for the contents of this message unless independently verified in writing or digitally certified. Any views or options presented are solely those of the author and do not necessarily represent those of XXXXXX unless otherwise specifically stated. You are hereby notified that if you have received this message in error any review, dissemination, distribution or copying of this message is unlawful and strictly prohibited, and you should, with normal business courtesy, immediately notify the sender of the incident and then destroy this message by deletion and removal from your Deleted Items folder. Any opinions, explicit or implied, are solely those of the author and do not necessarily represent those of XXXXXX group of companies.

2. DISCLAIMER

Questo documento contiene informazioni di proprietà XXXXXX e deve essere utilizzato esclusivamente dal destinatario in relazione alle finalità per le quali è stato ricevuto. E' vietata qualsiasi forma di riproduzione o di divulgazione senza l'esplicito consenso di XXXXXX. Qualora fosse stato ricevuto per errore si prega di in-

formare tempestivamente il mittente e distruggere la copia in proprio possesso.

3. DISCLAIMER

Le informazioni trasmesse sono da intendersi inviate solo ed esclusivamente alla persona alla quale sono state indirizzate e possono contenere materiale strettamente confidenziale e/o riservato. Qualsiasi utilizzo, ritrasmissione o diffusione delle presenti informazioni, anche solo parzialmente, sono proibite a tutte le persone od entità diverse dal destinatario. Se hai ricevuto queste informazioni per errore, contatta urgentemente il mittente e cancella immediatamente il materiale dal computer.

The information transmitted is intended only for the person or entity to. which it is addressed and may contain confidential and or privileged material. Any review, retransmission, dissemination or other use of, or taking of any action in reliance upon, this information by persons or entities other than the intended recipient is prohibited. If you received this in error, please contact the sender and delete the material from any computer.

Firma Fisica: è invalsa l'abitudine da parte di qualcuno di inserire uno *specimen* di *firma* (l'immagine della propria firma/fisica) nell'e-mail o negli allegati. Non va mai fatto! Bisogna sempre ricordare che il messaggio di posta elettronica è una cartolina postale che tutti possono leggere. Nessuno farebbe circolare il suo *specimen* di *firma,* ma potrebbe essere fatto, anche se sconsigliabile, solo ed esclusivamente se il messaggio viene inviato criptato tramite un sistema S/MIME con relativo certificato digitale ad un destinatario fidato e conosciuto.

Gestione degli invii di posta elettronica

L'invio di un messaggio di posta è un aspetto che va considerato con molta attenzione. Inviare un messaggio non significa avere la sicurezza matematica che venga ricevuto e soprattutto letto dal destinatario, qualsiasi sia il sistema di trasmissione.

Data ed Ora del messaggio

E' la parte fondamentale nel "non ripudio". Il fatto di poter sostenere di non avere ricevuto un messaggio o di averlo ricevuto in un giorno diverso o in un'ora diversa, dipende dal tipo di messaggio e dalla sua natura intrinseca. Si intuisce che una transazione di borsa deve partire ed arrivare entro un certo lasso di tempo: il concetto del tempo è ormai innato nella vita moderna ed ha ovviamente influenzato anche l'e-mail ed in genere tutto quello che avviene nella rete.
Non si parla più di enti che certificano un'ora ed una data, **ma di tecnologie che certificano**[47]. Questo concetto merita una riflessione: le tecnologie sono in continua evoluzione in questo settore e, vista l'importanza che ha l'omogeneità del tempo nelle comunicazioni e in tutta l'attività umana, è bene sapere che a poterla definire è solo la tecnologia. Non è né la PEC a poterla definire, né i gestori del servizio medesimo, tantomeno il CNIPA (Centro Nazionale per l'Informatica nella Pubblica Amministrazione), bensì la tecnologia.
Ecco un esempio: se si chiede ad un notaio di certificare l'ora, egli guarda l'orologio e dice che sono le 11:30 e lo certifica. Se si tratta di un notaio tecnologicamente avanzato, egli va nel sito del **Inrim**[48] e fa la stessa cosa, ma nel secondo caso usa una tecnologia corretta anche se ci sarà un minimo di scarto in secondi dal momento in cui rileva l'ora al momento in cui la certifica. Questa è la dimostrazione pratica che un essere umano non può certificare un dato tecnologico come il tempo.
L'intero complesso che regola data ed ora in tutti i server del mondo si basa su elementi coordinati da sistemi collegati tra loro. Tale sincronia rende immodificabili le informazioni relative all'ora e alla data, altrimenti ci sarebbe il caos.

Ecco alcuni esempi: il sistema tecnologico di un aereo (computer, server ecc.) che parte da New York e va a Roma, i treni nella loro percorrenza, gli scambi finanziari telematici di borsa e cambio ecc. funzionano, né più, né meno, come un messaggio e-mail, con diversi

[47] Legge 28 gennaio 2009, n. 2, art. 16/6 omissis…. *o analogo indirizzo di posta elettronica basato su tecnologie che certifichino data e ora dell'invio e della ricezione delle comunicazioni e l'integrità del contenuto delle stesse, garantendo l'interoperabilita' con analoghi sistemi internazionali.*

[48] http://www.inrim.it/ Istituto Nazionale di Ricerca Metrologica *(I.N.RI.M)*, Ora ufficiale ed anche ora legale con questo termine si intende l'anticipo di 60 minuti primi dell'ora del fuso di appartenenza per un periodo dell'anno stabilito per legge. Questo tipo di provvedimento fu proposto per la prima volta nel 1907 dal deputato inglese W. Willett e diventò legge (Daylight Saving Bill) in Gran Bretagna nel 1908

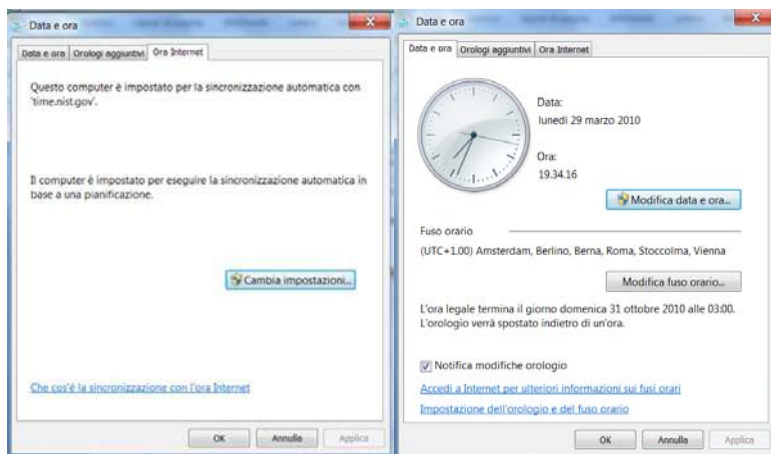
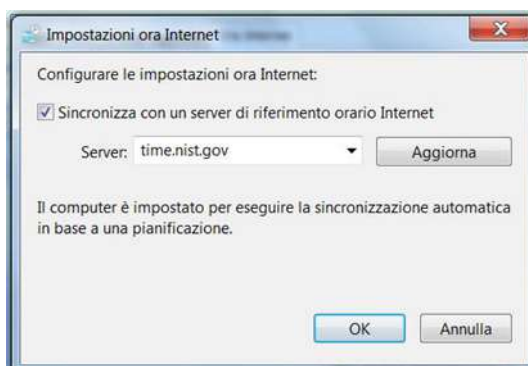
server che tracciano automaticamente la data e l'ora di partenza, di transito e di arrivo delle e-mail in tutto il suo percorso (in gergo **UTC**, *Coordinated Universal Time)*[49] ed è visibile oggi nell'orologio di tutti i PC e dei server, si chiama **"ora Internet"**. Questo è il frutto del collegamento di tutti i server che regolano ora e data in tutto il mondo attraverso gli NTP (National Time Provider), in Italia www.inrim.it , negli USA www.nist.gov e via dicendo**.** Attraverso una serie di orologi atomici che scandiscono il tempo in tutto il mondo e che non si fermano mai, si ottiene l'ora esatta nel fuso orario in cui si risiede. L'ora viene regolata e tutto funziona, senza bisogno di avere un notaio od un gestore PEC che la certifichi! E' la tecnologia che pensa a questo, automaticamente, con orologi atomici che non si fermano mai, fornendo così l'ora esatta nel fuso orario in cui si risiede.

Qualsiasi ente che dovesse certificare la data e l'ora di una transazione dovrà connettersi ad una di queste fonti tecnologiche e non guardare l'orologio che ha al polso. Quanto affermato dalla modifica della legge 28 gennaio 2009, n. 16/6 *"**o analogo indirizzo di posta elettronica basato su tecnologie che certifichino data e ora dell'invio e della ricezione delle comunicazioni e l'integrità del contenuto delle stesse, garantendo l'interoperabilita' con analoghi sistemi internazionali.**"* È, come l'ora atomica, rigorosamente esatta.

E' bene comunque controllare se l'orologio del nostro PC sia sincronizzato in modo corretto nella rete: è molto semplice, richiede solo pochi minuti ed una volta fatto avremo sempre un'ora rigorosamente esatta definita come "Ora Internet".

In Windows cliccare sull'orologio in basso a destra dello schermo e cliccare poi in : **"modifica impostazioni data ed ora".** Vi si aprirà questa finestra: cliccare su **"Ora Internet"**

---

[49] Il **tempo coordinato universale**, conosciuto anche come **tempo civile** e abbreviato con l'acronimo **UTC** (compromesso tra l'inglese *Coordinated Universal Time* e il francese *Temps universel coordonné*), è il fuso orario di riferimento da cui sono calcolati tutti gli altri fusi orari del mondo. Esso è derivato (e coincide a meno di approssimazioni infinitesimali) dal tempo medio di Greenwich (in inglese *Greenwich Mean Time*, GMT), e perciò talvolta è ancora chiamato GMT. Il nuovo nome è stato coniato per non dover menzionare una specifica località in uno standard internazionale. L'UTC si basa su misurazioni condotte da orologi atomici invece che su fenomeni celesti come il GMT. "UTC" non è una vera abbreviazione: è una variante di tempo universale, abbreviato in UT, e modificato con C (per "coordinato") come suffisso, per rafforzare l'idea che è quello adottato da tutti e per poter avere una codifica a 3 caratteri in modo da seguire lo standard per le indicazioni dei fusi orari (e.g.: CET per Central European Time in Europa, EST per Eastern Standard Time negli USA, etc).

Cliccare quindi su **"Cambia impostazioni"** qualora si voglia cambiare il sincronismo con il server di riferimento, che nella schermata è quello del NIST negli Stati Uniti. Non ha importanza dove il provider sia situato, in quanto, automaticamente verrà sincronizzato con il vostro fuso orario.

Conferma di ricezione e lettura

Attivare sempre la conferma di ricezione e lettura del messaggio. Questo non offre la sicurezza matematica che il messaggio sia stato ricevuto e letto, ma almeno si potrà insistere e magari provare in

giudizio la ricezione e lettura in special modo se ritorna indietro la conferma relativa.
Inviare sempre il messaggio per conoscenza a se stessi, perché così il sistema genererà in posta inviata "l'intestazione Internet" del messaggio con la "storia" di tutti i suoi passaggi, similmente alla ricevuta di ritorno di una raccomandata AR. Solo utilizzando il certificato digitale e la richiesta di conferma con protocollo S/MIME avrete la certezza matematica della ricezione del messaggio da parte del server del provider del ricevente analogamente alla PEC.

LA SCELTA, PROTEZIONE ED USO DELLE PASSWORD

Per proteggere il proprio PC, ma anche l'accesso ad alcuni file e senz'altro all'account di posta elettronica, sia esso di tipo client, che a maggior ragione in quello di tipo WEB nel server del vostro provider di posta elettronica, dovrete far fronte al problema amletico della password.
Le password rappresentano le chiavi di accesso alle informazioni personali inserite nel proprio computer e negli account online.
Se riescono a sottrarre queste informazioni, hacker o utenti malintenzionati possono utilizzare il tuo nome per aprire nuovi conti di carte di credito, accendere un mutuo o assumere la tua identità in transazioni online. Spesso gli attacchi diventano evidenti solo quando ormai è troppo tardi.
Usare per la password parole che sono vicine alla propria sfera personale tipo, data di nascita, nome dei propri familiari e simili sono assolutamente da evitare non servirebbero a nulla, del resto è sempre più difficile in un mondo fatto di PIN e password, ricordare altre password a memoria esistono metodi per creare password complesse e mantenerle segrete.

Cosa rende una password complessa

A un malintenzionato, una password complessa deve apparire come una stringa casuale di caratteri. I seguenti criteri possono essere di aiuto per la creazione di una password difficile da identificare:
Lunghezza adeguata. Ogni carattere, numero o carattere "speciale" (* + @ ecc.) che si aggiunge alla password contribuisce ad aumentare la protezione. La password dovrebbe contenere un minimo di 8 caratteri; la lunghezza ideale è dai 14 caratteri in su.

Molti sistemi supportano anche l'uso di spazi nelle password ed è quindi possibile creare una frase composta da più parole (una "*passphrase*") cioè una frase che sostituisca la password; qualora il sistema non consenta degli spazi si può sostituire gli stessi con un segno tipo _ "*underscore*". Una passphrase è più semplice da ricordare rispetto a una singola password, oltre che più lunga e più difficile da indovinare, bisognerà però evitare luoghi comuni ad esempio se la *passphrase* è un detto di una persona nota, la stessa potrà essere individuata facilmente, difatti gli hackers quando riescono ad individuare che la password è una *passphrase,* con molta facilità passeranno al setaccio i più famosi modi di dire, facilmente reperibili anche nel web, sarà allora un gioco da ragazzi scoprire la vostra *passphrase* .

Combinazione di lettere, numeri e simboli. Più sono diversi i caratteri utilizzati per la password, più difficile sarà indovinarla. È inoltre importante ricordare che:

- Meno sono i tipi di caratteri utilizzati nella password, più è importante aumentarne la lunghezza. Una password di 15 caratteri composta solo da numeri e lettere casuali è 33.000 volte più complessa rispetto a una password di 8 caratteri composta da caratteri disponibili sulla tastiera, in questo caso la tabella dei codici ASCII[50] vi sarà di grande aiuto. Se non è possibile creare una password che contenga simboli, per ottenere lo stesso livello di protezione è necessario aumentarne la lunghezza. Una password ideale è lunga e contiene tipi di simboli diversi.
- Utilizzo dell'intera tastiera e non solo dei caratteri più comuni. I simboli che si ottengono tenendo premuto il tasto "MAIUSC" e digitando un numero sono molto comuni nelle password. La password è molto più efficace quando si sceglie tra tutti i simboli a disposizione sulla tastiera, compresi i segni di punteggiatura presenti sulla riga superiore e i simboli caratteristici della propria lingua.

Utilizzo di parole e frasi facili da ricordare, ma difficili da indovinare per gli altri. Il modo migliore per ricordare le proprie password e passphrase è annotarle. Al contrario di quanto si pensa comunemente, non c'è nulla di sbagliato nell'annotare le proprie password, purché siano conservate in un luogo sicuro.

[50] **ASCII** è l'acronimo di **A**merican **S**tandard **C**ode f or **I**nformation **I**nterchange (ovvero *Codice Standard Americano per lo Scambio di Informazioni*), http://it.wikipedia.org/wiki/ASCII

Le password sono più al sicuro da Internet, se scritte su un pezzo di carta, piuttosto che memorizzate in un software di gestione delle password, su un sito Web, o con altri strumenti di memorizzazione.

Creazione di una password complessa e semplice da ricordare in 6 passaggi

Per creare una password complessa, ecco una procedura da seguire:

1. Pensare a una frase semplice da ricordare. Questo è il punto di partenza per creare una password o *passphrase* complessa. Usare una frase semplice da ricordare, ad esempio "Mio figlio Antonio ha tre anni".
2. Verificare se il computer o il sistema online supporta le passphrase. Se possibile, utilizzare una passphrase (con spazi tra i caratteri) sul computer o sul sistema online.
3. Se il computer o il sistema online non supportano le *passphrase*, convertirle in password. Prendere la prima lettera di ciascuna parola della frase per crearne una nuova che non avrà alcun senso. Utilizzando l'esempio precedente, si otterrà: "mfAhta".
4. Rendere la password ancora più complessa usando lettere maiuscole e minuscole alternate a numeri. È utile a tal fine spostare le lettere o scrivere parole con errori ortografici. Nella passphrase composta in precedenza, ad esempio, si può provare a scrivere il nome Antonio con qualche errore oppure sostituire la parola "tre" con il numero 3. Le sostituzioni possibili sono molte e a una frase più lunga, come detto, corrisponderà ad una maggiore complessità. La passphrase potrebbe diventare "Mio FigliO Ant3A ha 3 anNi". Se il computer o il sistema online non supporta le passphrase, utilizzare la stessa tecnica per creare una password più breve. La password, in questo caso, potrebbe essere "MfAh3a".
5. Infine, sostituire alcuni caratteri con simboli speciali. È possibile utilizzare simboli simili a lettere, combinare le parole (rimuovere spazi) e rendere in altri modi la password più complessa. Grazie a queste elaborazioni, si crea una passphrase del tipo "MioFigliO 8A h@ 3 @nni" o una password (utilizzando la prima lettera di ciascuna parola) "MF8h3@".
6. Valutare sempre l'efficacia della nuova password con uno strumento di controllo delle password eccone un paio uno della

MICROSOFT[51] ed un altro di PASSWORDMETER[52], ma potrete reperirne molti altri con una semplice ricerca on-line. Lo strumento di controllo delle password è una funzione, che non registra le informazioni, disponibile sul sito Web e in grado di verificare l'efficacia delle password utilizzate.

1. Esistono poi dei software che creano dei veri e propri algoritmi da usare per la creazione di password complesse.

Strategie da evitare

Alcuni metodi utilizzati per creare le password sono molto prevedibili per i malintenzionati, ricordate che per gli hackers indovinare una password è una sorta di sfida ed un punto d'onore.

Per evitare di creare password semplici da indovinare ecco alcuni piccoli suggerimenti:

- Evitare sequenze o caratteri ripetuti. Password simili a "12345678", "222222", "abcdefg" o composte da lettere adiacenti sulla tastiera sono molto semplici da indovinare, tipica è qwerty la prima serie di lettere della tastiera.
- Evitare sostituzioni di caratteri con numeri o simboli simili. Gli utenti malintenzionati sono abbastanza abili a decifrare una password. Non si lasceranno ingannare da sostituzioni con caratteri simili, ad esempio della lettera "i" con il numero "1" o della lettera "a" con il simbolo "@", come in "M1cr0$0ft" o "P@ssw0rd". Sistemi simili risalgono ai tempi di Giulio Cesare[53] ma all'epoca non c'erano computer. Queste sostituzioni possono essere efficaci se combinate con altre misure di protezione, quali la lunghezza, gli errori ortografici o le variazioni da maiuscole a minuscole, che contribuiscono a rendere più complessa la password.
- Non utilizzare il nome di accesso. Non è consigliabile utilizzare come password una parte del proprio nome, la data di nascita, il codice fiscale o altre informazioni simili. Questi sono i primi tentativi messi in atto da un utente malintenzionato come già accennato in premessa.

[51] http://www.microsoft.com/italy/athome/security/privacy/password_checker.mspx
[52] http://www.passwordmeter.com/
[53] Il **cifrario di Cesare** è uno dei più antichi algoritmi crittografici di cui si abbia traccia storica. È un cifrario a sostituzione monoalfabetica in cui ogni lettera del testo in chiaro è sostituita nel testo cifrato dalla lettera che si trova un certo numero di posizioni successive nell'alfabeto. http://it.wikipedia.org/wiki/Cifrario_di_Cesare

- Non utilizzare parole presenti sul vocabolario di una qualsiasi lingua. Gli utenti malintenzionati utilizzano strumenti sofisticati in grado di indovinare rapidamente le password composte da parole presenti in più dizionari, anche se con errori di ortografia, scritte al contrario o con sostituzioni. Tra queste sono comprese anche parole irriverenti o parole che non si pronuncerebbero mai in presenza dei propri figli.
- Non utilizzare la stessa password per più account. Se uno dei computer o sistemi online che utilizzano la password in questione viene attaccato, anche tutte le informazioni protette dalla stessa password saranno compromesse. È fondamentale utilizzare password diverse per ciascun sistema.
- Non utilizzare gli archivi online. Se gli utenti malintenzionati trovano le password memorizzate online o su un computer in rete, avranno accesso a tutte le informazioni protette con le medesime password.

La "password vuota" e Microsoft

Una password vuota (nessuna password) in un account è più sicura di una password simile a "1234". Gli utenti malintenzionati possono facilmente indovinare una password semplice, ma sui computer che utilizzano Windows XP, un account senza password non è accessibile in remoto da una rete o da Internet (l'opzione non è disponibile per Microsoft Windows 2000, Windows Me o versioni precedenti). È possibile scegliere una password vuota per l'account del computer quando vengono soddisfatti i seguenti criteri:

- Si utilizza un solo computer o diversi computer, ma non è necessario accedere alle informazioni di un computer da un altro;
- Il computer si trova in un luogo sicuro (coloro che hanno accesso al computer sono persone fidate).

L'uso di una password vuota non è sempre una buona idea. Ad esempio, un computer portatile utilizzato in luoghi diversi probabilmente non è sempre al sicuro ed è quindi consigliabile utilizzare in questo caso una password complessa.

Accesso e modifica delle password

Account online

Per i siti Web esiste una vasta gamma di criteri con cui si stabilisce come accedere agli account e modificarne le password. Cercare un

collegamento (ad esempio "Account") nella home page del sito, mediante il quale accedere all'area speciale in cui gestire le password e gli account.

Password del computer

I file della Guida online del sistema operativo forniscono in genere informazioni su come creare, modificare e accedere agli account utente, protetti da password e su come richiedere la protezione mediante password all'avvio del computer. È possibile trovare queste informazioni anche nel sito Web del produttore del software. Ad esempio, se si utilizza Microsoft Windows XP, nella Guida online (in inglese)[54] è possibile trovare informazioni su come gestire le password (in inglese)[55], modificare le password (in inglese)[56] e molto altro ancora.

Segretezza delle password

Utilizzare password e passphrase con la stessa attenzione con cui si utilizzano le informazioni che protegge.

- Non rivelare a nessuno password o passphrase. Non rivelare le password ad amici o parenti (specialmente ai bambini) che possono divulgarle ad altre persone meno affidabili. Le password da condividere con altre persone, ad esempio la password del proprio conto in banca online da condividere con il proprio coniuge, può rappresentare un'eccezione.
- Proteggere le password registrate. Prestare attenzione al luogo in cui si conservano le password registrate o annotate. Non lasciare le stesse in luoghi in cui non si lascerebbero le informazioni protette dalle password.
- Non inviare la password tramite posta elettronica anche se in risposta ad una richiesta arrivata via posta elettronica. Qualsiasi messaggio di posta elettronica in cui viene richiesta la propria password o viene indicato un sito Web da visitare per verificare la propria password, è spesso un tentativo di frode. Tra questi messaggi spesso vi sono richieste di aziende o persone ritenute atten-

[54] http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/default.mspx
[55] http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/usercpl_manage_passwords.mspx
[56] http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/windows_password_change.mspx

dibili. La posta elettronica può essere intercettata quando è in transito e i messaggi che richiedono informazioni personali, possono non provenire dal mittente indicato. Le frodi tramite "phishing" in Internet vengono attuate mediante messaggi di posta elettronica falsificati, che inducono un utente a rivelare il proprio nome e le proprie password per rubarne l'identità.

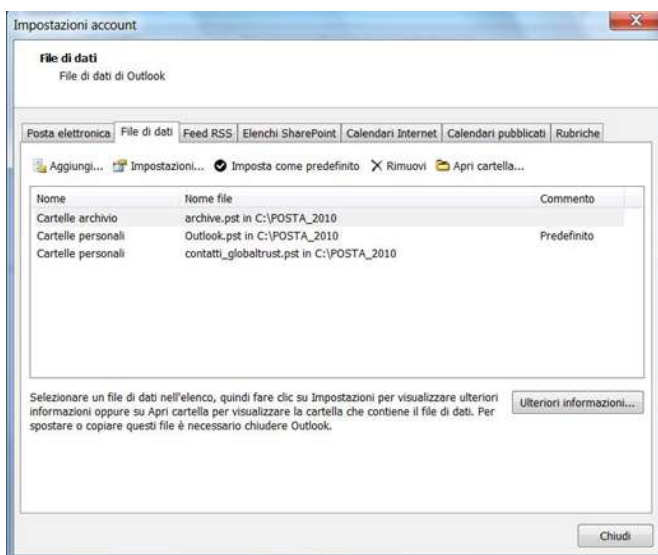
- Modificare le password con regolarità. In questo modo è possibile tenere alla larga hacker e altri utenti malintenzionati. La complessità della password contribuisce a renderla sicura per molto tempo. Una password che contiene meno di 8 caratteri può essere utilizzata per una settimana circa, mentre una password con 14 o più caratteri (che segue le regole suddette) può essere utilizzata per molto tempo.
- Non digitare la password in computer sui quali non si ha il diretto controllo. I computer disponibili in InternetCafé, laboratori informatici, sistemi condivisi, sale conferenze e sale di aspetto di un aeroporto non devono essere considerati sicuri per uso personale, ma solo per navigare in Internet in modo anonimo. Non utilizzare questi computer per controllare la posta elettronica, accedere a chat room, verificare l'estratto conto bancario, controllare la posta aziendale o altri account che richiedono nome utente e password. Gli utenti malintenzionati possono acquistare a costi minimi alcuni dispositivi molto semplici da installare che registrano la sequenza dei tasti digitati. Questi dispositivi consentono ai malintenzionati di ottenere tramite Internet tutte le informazioni digitate sulla tastiera di un computer. Password e passphrase hanno la stessa importanza delle informazioni che proteggono.

Cosa fare se la password viene rubata

Controllare regolarmente tutte le informazioni protette da password, ad esempio gli estratti conto di fine mese, i report di credito, gli account di acquisti online.

L'uso di password complesse e facili da ricordare consentono di migliorare la protezione contro frodi e furti di identità, ma non offre garanzie assolute. Indipendentemente dalla complessità, se qualcuno riesce a infiltrarsi nel sistema in cui è archiviata la password, potrà disporne liberamente. Se si sospetta, che qualcuno sia riuscito ad accedere alle proprie informazioni, rivolgersi immediatamente alle autorità competenti.

LA PORTABILITA' DEI DATI DELLA PROPRIA CASELLA DI POSTA ELETTRONICA

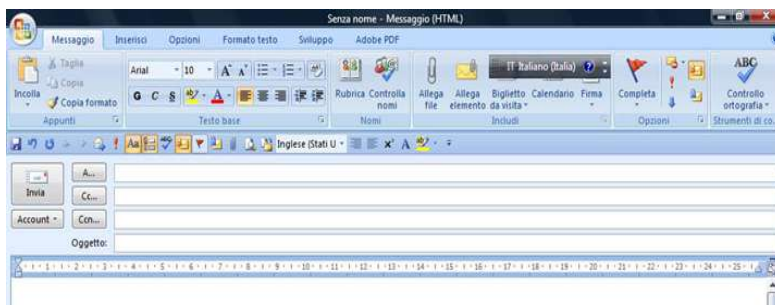
Come si è visto, attraverso il provider della propria casella di posta elettronica si può avere a disposizione la stessa con tutto il contenuto in qualsiasi parte del mondo, si è altresì visto che, oltre a problemi di capienza, ci sono anche problemi di sicurezza, privacy e di backup dei propri dati, nonché la necessità di poter disporre di caselle di posta elettronica in luoghi sicuri, inaccessibili, ma allo stesso tempo fruibili. I messaggi di posta elettronica sono normalmente archiviati attraverso un formato apposito. Non è possibile la normale gestione dei file nei programmi come Microsoft Outlook, detti .pst, che usano sistemi di Import/Export della casella di posta elettronica, che risiedono su di una cartella specifica nel proprio PC, come da immagine che segue:

Questa cartella può essere sostituita con un'altra a scelta, usando anche supporti portatili come chiavette USB. Sarà quindi sufficiente archiviare i dati nella USB in modo che la stessa sia fruibile, sia con il PC di casa/ufficio, che con qualsiasi portatile, ovviamente dovrà essere configurato con gli stessi parametri. La portabilità sarà così

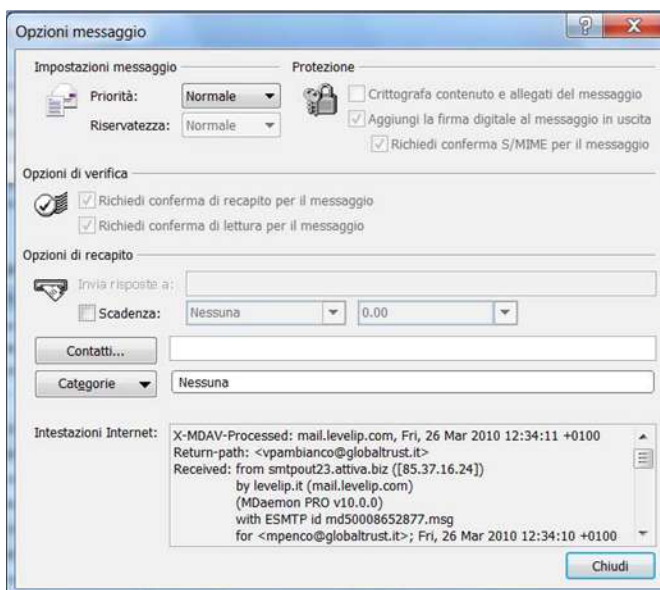
assicurata, l'unico inconveniente sarà la perdita della USB. Una procedura importante sarà quella di assicurarsi una copia della cartella dove è contenuta la posta elettronica e la protezione dell'accesso alla USB con password. Ci sono inoltre in commercio chiavette USB provviste di sofisticati sistemi di protezione che garantiscono l'inviolabilità della stessa.

IL MESSAGGIO DI POSTA ELETTRONICA NEI DETTAGLI

Il messaggio di posta elettronica è composto da due parti principali: intestazione del messaggio e corpo del messaggio. La prima è altresì divisa in due parti: l'intestazione normale, quella visibile a tutti, e quella avanzata che raccoglie tutte le informazioni relative al messaggio stesso.

Intestazione del messaggio. Come in una comune lettera il messaggio di posta elettronica possiede l'intestazione di chi spedisce il messaggio e cioè l'indirizzo di posta elettronica del mittente; l'indirizzo del destinatario/i al quale viene inviato il messaggio, contrassegnato con A; l'indirizzo/i di altri destinatari per conoscenza, viene contrassegnato con CC.
L'indirizzo del destinatario/i a cui il messaggio viene inviato per conoscenza "nascosta", viene contrassegnato con CCn e usato qualora si voglia inviare il messaggio ad altri senza però far vedere al destinatario principale ed agli eventuali CC, per conoscenza, che lo si è fatto.

L'oggetto del messaggio. Questa parte a volte è lasciata in bianco. Non bisogna mai farlo, in quanto molti filtri antispam scartano sia a livello di server sia a livello di PC, tutti i messaggi privi di OGGETTO.
Ecco un tipico esempio di intestazione (header) di un messaggio di posta elettronica (lo spazio bianco sotto l'intestazione è quello riservato al corpo del messaggio):

L'intestazione Internet (header) del messaggio avanzata o completa

E' la parte vitale del messaggio di posta elettronica in qualsiasi modo venga inviato e ricevuto, rappresenta la storia ed il percorso del messaggio stesso e potrà essere usato in caso di contestazione. Vediamo come ricavarlo, esaminando solamente il client di posta Outlook 2007, poiché negli altri la procedura è similare. In posta ricevuta cliccare con il pulsante destro del mouse sulla linea del messaggio interessato e apparirà la schermata che segue:

Cliccare con il pulsante destro del mouse nell'interno di: **Intestazione Internet e** apparirà una nuova finestra. Cliccare su: **seleziona tutto e** a questo punto si potrà incollare tutto il contenuto dell'Intestazione Internet (header del messaggio) in qualsiasi Word Processor con il risultato che segue:

Return-Path: scrivimi@rossi.it tracciamento di ritorno del messaggio
Delivered-To:cittadinInternet.org-mpenco@cittadinInternet.org consegnato a:
Received: (qmail 16876 invoked by uid 107); 3 Aug 2009 11:40:32 -0000 ricevuto da: e l'user identifier o **UID** è il numero che identifica univocamente un utente del sistema
X-Spam-Checker-Version: SpamAssassin 3.2.5 (2008-06-10) on hobbes.impulso.it la versione del sistema antispamming residente nel server
X-Spam-Level: l'eventuale livello di spamming
X-Spam-Status: No, score=0.0 required=5.0 tests=none autolearn=disabled version=3.2.5 Lo status d'intervento dell'anti spamming in caso di messaggio spam
Received: from hermes.teseo.it (213.92.8.50) Il messaggio è stato ricevuto da un server denominato hermes.teseo.it identificato dal suo identificativo IP by vmx1 with ESMTPS (DHE-RSA-AES256-SHA encrypted); 3 Aug 2009 11:40:24 -0000 Il server ha provveduto ad identificare che il messaggio è firmato attraverso una chiave a 256 bit
Received-SPF: pass (vmx1: SPF record at pinobruno.it designates 213.92.8.50 as permitted sender) **Sender Policy Framework** è il sistema per limitare gli abusi nella posta elettronica dove viene predeterminato il mittente autorizzato a spedire il messaggio ed altro. Il sistema è piuttosto complesso ed ancora studiato da: **http://www.openspf.org**
Received: (qmail 27568 invoked from network); 3 Aug 2009 13:40:39 +0200 data e ora di ricezione del messaggio
Received: from 93-43-156-184.ip92.fastwebnet.it (HELO pinocasa) (93.43.156.184) by hermes.teseo.it with SMTP; 3 Aug 2009 13:40:37 +0200. Qui vengono chiaramente indicate come i server dei provider si scambiano automaticamente informazioni relative al messag-

gio identificandosi con il proprio indirizzo IP HELO e il sistema di mutuo riconoscimento dei server usato dal protocollo SMTP

From: "Luca Rossi" scrivimi@dominio.it In questo caso il messaggio è stato inviato a più destinatari

To: "Massimo F.Penco" <mpenco@cittadinInternet.org>, "Marco Sciascia" <sciascia@sciascia.it>

Cc: "Franz Bianchi \(franz.bianchi@bianchi.it\)" franz@gmail.com

References: Riferimenti univoci del messaggio !AAAAAAAAAAYAAAAAAAAAJqvr/97qgtMorfeQLOmxhXCgAAAEAAAAJU-laZ0gnG9Moujl/FXUO2IBAAAAAA==@cittadinInternet.org le referenze univoche relative al messaggio.

In-Reply-To: !&!AAAAAAAAAAYAAAAAAAAAJqvr/97qgtMorfeQLOmxhXCgAAAEAAAAJU-laZ0gnG9Moujl/FXUO2IBAAAAAA==@cittadinInternet.org la risposta con codice univoco relativo al messaggio.

Subject: R: LINK L'oggetto del messaggio

Date: Mon, 3 Aug 2009 13:40:08 +0200 La data e l'ora prelevata dall'ultimo server con l'adeguamento al fuso orario locale

Message-ID: <!&!AAAAAAAAAAYAAAAAAAAAJgFn/NeBRRJi7QWeNbLzJLCgAAAEAAA-AH2+6P0GZYhFioA0GvLoes8BAAAAAA==@pinobruno.it> Il messaggio a questo punto viene fornito di un identificativo univoco che viene unito all'indirizzo del destinatario

MIME-Version: 1.0 La versione del protocollo di trasmissione del messaggio

Content-Type: application/x-pkcs7-mime; l'applicazione con cui è stato firmato il messaggio

smime-type: signed-data il tipo di firma del messaggio usata dal protocollo di trasmissione smime

Name: "smime.p7m" il nome del file di firma, suo identificativo

Content-Transfer-Encoding: base64 Il codice di trasferimento del testo del messaggio

Content-Disposition: attachment l'avviso che il messaggio contiene allegati

Filename:"smime.p7m" il nome protocollo del file usato per la firma del messaggio
X-Mailer: Microsoft Office Outlook 12.0 il software usato per il servizio di posta elettronica
Thread-Index:AcoUG6TSCWUQHzvlTeSofK8/dGowkAAE0RCg Identificativo dell'indicizzazione del messaggio di posta nel suo percorso
Content-Language: it la lingua usata.
Disposition-Notification-To: "Luca Rossi" scrivimi@dominio.it la disposizione data dal mittente a chi deve essere inviata l'e-mail.
X-Antivirus: avast! (VPS 090802-0, 02/08/2009), Inbound message Il tipo di Antivirus e versione nonché la data di aggiornamento e numero del data base usato dall'antivirus del messaggio in "transito".
X-Antivirus-Status: Clean lo "status" del messaggio in questo caso "clean" privo di virus.

NOTE:
In blu (grassetto) è riportato l'esatto corpo dell'header, in nero le spiegazioni relative.

LINK nelle E-MAIL

Da parte di tutti ormai, c'è il timore dei link ricevuti tramite e-mail, possono condurre in situazioni poco piacevoli (phishing) ed altro. È bene quindi diffondere l'utilizzo di software come **GlobaltrustCallingID LinkAdvisor**[57] che permette di conoscere preventivamente la pagina web che si andrà a "navigare", una volta posizionato il mouse (senza cliccarlo) sul link che arriva tramite e-mail.

Allegati al messaggio

A volte è necessario inviare messaggi con grandi files allegati. Bisogna ricordare di usare con parsimonia lo spazio altrui, si potrebbe intasare e/o bloccare la casella di posta di colui con il quale state corrispondendo, con le ovvie conseguenze.
In questi casi, si deve usare un diverso sistema di posta come il **GlobaltrustCertifiedMail**[58] che consente, nella versione Corporate, di inviare anche 4 GB di allegati. Vi sono anche numerosi altri sof-

[57] http://www.callingid.it/
[58] http://www.certifiedmail.it/

tware gratuiti in grado di fare ciò, ma bisogna fare molta attenzione nella scelta degli stessi.

PROTEZIONE DELLA POSTA ELETTRONICA E RELATIVI ALLEGATI

Con l'avvento della PEC (Posta Elettronica Certificata), sicuramente si è iniziato un cammino che renderà più semplice la corrispondenza e tutte quelle incombenze che fino ad oggi erano affidate alla raccomandata con ricevuta di ritorno (avviso di ricevimento), ancora oggi largamente usata, ma spesso, fonte di contestazioni anche di natura legale.

RAFFRONTI E COMPARAZIONI CON GLI ALTRI SISTEMI DI TRASMISSIONE ED INVIO DOCUMENTI (RACCOMANDATE, FAX, PEC)

È d'obbligo un breve confronto con gli altri sistemi fisici ed elettronici di invio documentazione.

Qualche cenno sulla ormai obsoleta Raccomandata AR

È ormai diffusamente riconosciuto che l'invio della raccomandata AR non è la soluzione ai problemi di seguito elencati:

1) La certezza della ricezione;
2) Il "non ripudio" della ricezione;
3) I contenuti della stessa (che possono essere anche fogli bianchi);
4) L'ora e la data di ricevimento.

Vi è infatti giurisprudenza consolidata,[59] che quello che veniva considerato un sistema sicuro in effetti non lo è.

La certezza della ricezione: la raccomandata si può perdere e non arrivare a destinazione e questo può avvenire a maggior ragione per la ricevuta di ritorno che viaggia con posta ordinaria.

Il "non ripudio" della ricezione: sulla base di quanto esposto, chiunque può affermare di non aver ricevuto la posta, o manca uno dei due requisiti, o una combinazione dei due. Può verificarsi la si-

[59] http://www.globaltrust.it/seclaw/italia/postaCert/index.aspx

tuazione che Bruno riceva la raccomandata, ma Anna non abbia la ricevuta di ritorno.

I contenuti della raccomandata: non vengono in alcun modo garantiti. Conseguentemente, l'invio di una busta vuota fa sì che Anna riceva un avviso di ricevimento da Bruno di una busta, che non contiene nulla. La panacea dell'invio, nel cosiddetto foglio busta, con il timbro postale nel primo foglio inviato, risolve parzialmente il problema. Infatti, assieme al primo foglio, potrebbero essere inseriti degli altri che non vengono validati dal timbro postale. La conferma di averli inviati e ricevuti è vanificata.

L'ora di ricevimento: non è garantita. Una volta il postino faceva firmare la ricevuta con l'ora di ricezione, tratta ovviamente da un orologio, il vostro e/o quello del postino, che non costituivano prova alcuna.

L'onere della prova spetta a: colui che riceve la raccomandata. Fortunatamente le più recenti sentenze della Corte di Cassazione hanno rivisto questo orientamento, anche se a volte in modo contrastante.
Alcune sentenze:[60]
(http://www.globaltrust.it/seclaw/italia/postaCert/index.aspx)
E' utile a questo punto fare un paragone fra la PEC e la Raccomandata AR ed il contrario, e tra PEC e S/Mime.

RACCOMANDATA A.R.	PEC
La raccomandata si può inviare in tutto il mondo senza limitazioni	Non esiste altro sistema simile al mondo, la PEC è interoperabile solo con se stessa
Nessuna garanzia sul contenuto della raccomandata	Stessa cosa nessun miglioramento
Smarrimento	Tecnicamente quasi impossibile lo smarrimento
Possibilità di Ripudio dei contenuti	Possibilità di Ripudio dei contenuti

[60] http://www.globaltrust.it/seclaw/italia/postaCert/index.aspx

Smarrimento della ricevuta di ritorno	Tecnicamente quasi impossibile lo smarrimento
Viene recapitato un avviso di giacenza al mittente	L'avviso di giacenza è recapitato nel PC del mittente solo se in funzione e connesso, altrimenti rimane nel server del provider
Il ricevente deve recarsi all'ufficio postale per ritirare la raccomandata	Il ricevente deve accedere al PC e connettersi per verificare se ci sono messaggi PEC per lui
Il mittente riceve indietro la raccomandata integra con l'annotazione di compiuta giacenza	Il mittente deve accedere al PC, connettersi per verificare se ci sono messaggi PEC di mancato ricevimento od anomalie nella spedizione/ricezione dei messaggi
Nel caso di compiuta giacenza la raccomandata viene restituita integra al mittente, nulla rimane all'ufficio postale. La documentazione, ricevute, ecc. sono a disposizione del mittente per un periodo di tempo praticamente illimitato. Non ci sono limiti nella spedizione o ricezione di raccomandate	Il messaggio con tutto il suo contenuto rimane nei server del ricevente per almeno 30 mesi, la legge non stabilisce cosa il gestore debba fare dei messaggi dopo i trenta mesi e neanche cosa deve fare se la casella di posta PEC risulta piena, tecnicamente la stessa rifiuta nuovi messaggi se piena, in modo automatico
Non esiste alcuna limitazione sul numero delle raccomandate che si possono fare	I provider offrono il servizio con limitazione dello spazio della propria casella di PEC, non esistono al momento disposizioni di legge che regolino cosa accade se lo spazio viene superato, cosa del resto molto probabile, dovendo il provider conservare per 30 mesi tutti i messaggi inviati
Esistono altri sistemi in Italia ed altri ancora nel mondo per l'invio di Raccomandate (raccomandata elettronica[61]), che evitano spostamenti verso gli uffici postali	Il costo della PEC non è poi così vantaggioso. A monte ci si deve dotare di Computer, collegamento ad Internet ed altro ancora

[61] http://www.poste.it/online/postaraccomandataonline/

S/MIME	PEC
E' lo standard universalmente riconosciuto in tutto il mondo per la trasmissione sicura della posta elettronica	Non è uno standard: per avere effetto e validità legale solo in Italia, il mittente e il destinatario debbono avere una casella di posta elettronica PEC
È il protocollo di trasmissione sicura, di qualsiasi genere di messaggio usato, con qualsiasi Client e-mail in tutto il mondo. Necessita di un certificato digitale di firma	Non è un protocollo di trasmissione ma un software di gestione di caselle di posta, inventato in Italia
Firma il messaggio ed i suoi allegati che divengono immodificabili e rimangono integri durante tutto il tragitto	Usa lo stesso protocollo S/MIME con il quale i gestori firmano "la busta di trasporto" ignorando i contenuti della stessa,
Il certificato digitale è, e rimane di proprietà del titolare dell'indirizzo e-mail con il quale è stato acquisito ed usato, a discrezione dello stesso, non solo per firmare messaggi di posta elettronica, ma anche qualsiasi documento in formato digitale	Il certificato di firma è di proprietà dei gestori, lo stesso non è univoco per ogni "busta di trasporto", l'uso di password e la disponibilità è a discrezione del gestore PEC, con un solo certificato possono essere firmate buste di trasporto di un numero indefinito di utenti del servizio PEC.
Il protocollo S/MIME può criptare il messaggio e-mail. Criptando lo stesso, oltre a rimanere integro, potrà essere letto solo dal mittente e dal destinatario	Il contenuto della "busta di trasporto" viaggia in chiaro. Una volta aperta, il contenuto può essere, letto, cancellato e modificato. L'unica cosa che ha in mano il mittente è la ricevuta della busta di trasporto, che nel suo tragitto, fino al PC del ricevente, è senz'altro rimasta integra, può essere però soggetta a procedure di sequestro da parte dell'AG .
Gli unici che hanno la possibilità di aprire un messaggio e suoi allegati inviati come su descritto sono il mittente	Sia il gestore di PEC del mittente, che il ricevente, avendo loro le credenziali ed il certifi-

ed il ricevente proprietari dei rispettivi certificati digitali.	cato digitale, hanno la possibilità di aprire la busta di trasporto e fare qualsiasi cosa dei messaggi e loro allegati
Di per se, il sistema di trasporto messaggi con protocollo S/MIME, da sufficienti garanzie di tracciamento dei messaggi, che passano attraverso una serie di server che sono ormai tutti connessi a sistemi NTP sincronizzati fra loro in tutto il mondo.	Il mittente deve accedere al PC e connettersi per verificare se ci sono messaggi PEC, di mancato ricevimento od anomalie nella spedizione del messaggio, la stessa cosa deve essere fatta dal destinatario
Il “non ripudio” dell’intero messaggio è assolutamente garantito	Garantisce solo il ricevimento della busta di trasporto che può contenere qualsiasi cosa.

Qualche cenno sulla storia del fax

1986, Il Fax

Intorno alla metà degli anni Ottanta, anche in Italia e nei principali uffici postali, iniziava l'era del Fax o facsimile. L'apparecchiatura era stata inventata oltre cent'anni prima, nel 1843, dallo scozzese Alexander Bain (1818-1903) ed era in grado di inviare immagini sulle linee telegrafiche. La tecnologia venne perfezionata dall'abate Giovanni Caselli, che nel 1856 presentò il Pantelegrafo. Nel 1865 iniziò, in Francia, il primo servizio pubblico di fax tra Parigi e Lione. Nel 1966 venne introdotto negli Stati Uniti lo standard EIA-328, poi ribattezzato Gruppo 1, che permetteva di scambiarsi documenti utilizzando fax di costruttori diversi. Nel 1978 furono introdotte le specifiche del Gruppo 2 e finalmente, nel 1980, apparve il Gruppo 3, che è tuttora lo standard usato dal Fax. Ancora oggi è possibile l'uso del fax presso gli uffici postali (nell'immagine telecopier Italtel HF del 1976; telecopiatrice Italtel GR2 del 1982).

La storia del fax ci fa capire come sia più lungo e difficile creare standard e interoperabilità rispetto all'invenzione, all'introduzione e all'utilizzo di un nuovo sistema; oltre 100 anni per un sistema di trasmissione accettabile.

Il FAX inventato nel 1843 e' stato utilizzato a partire dal 1980.
Questo dimostra che è molto più difficile mettere d'accordo i sistemi ed uniformare uno standard, che inventare un prodotto.
La trasmissione tradizionale via FAX è effettuata tramite connessione punto-punto, non da nessuna garanzia di sicurezza nemmeno di affidabilità e di certezza di ricezione di un messaggio, se si pensa poi che alcuni anni fa la carta usata era di tipo chimico e sbiadiva in pochissimo tempo, dimostrando come era inaffidabile qualsiasi prova nel tempo con questo sistema. Oggi, il FAX viene per lo più trasmesso con sistemi simili alle e-mail ed è quindi assolutamente equiparabile a queste ultime. Ciò nonostante, mentre alcune sentenze del

Consiglio di Stato lo definiscono come sistema **“universalmente accettato”**, contemporaneamente viene messa in cantiere la PEC, quando la comunicazione FAX ormai, è assimilabile ad una semplice e-mail. **Che fine ha fatto il vecchio Fax e la vecchia trasmissione FAX?**
Nelle moderne aziende si è evoluto in una comunicazione attraverso Internet, usando gli stessi protocolli e sistemi di un’e-mail, pochi di noi se ne sono accorti, forse ad eccezione degli addetti ai lavori all’interno delle aziende e dei professionisti del settore.

I motivi dell’evoluzione del FAX, da un sistema di trasmissione punto-punto ad un più moderno sistema, che è praticamente identico all’invio della posta elettronica.
I costi - I dati vengono trasmessi a pacchetto e non più punto-punto, cioè non da un apparato all’altro tramite linea telefonica, con le stesse identiche peculiarità di base delle e-mail. Questa è la prova che la tecnologia avanza comunque e non aspetta leggi o sentenze per evolversi.

FAX = E-mail

Cioè trasmissione elettronica di documenti siano essi testi, disegni, immagini foto ecc.

Ecco alcune interessanti sentenze che determinano in Italia come il FAX sia: uno standard di comunicazione universalmente accettato
E’ bene leggere le tre importanti sentenze del Consiglio di Stato che hanno definitivamente stabilito cosa è universalmente accettato nella trasmissione di documenti in Italia, le cui definizioni sono a dir poco inquietanti:

"Il fax rappresenta uno dei modi in cui può concretamente svolgersi la cooperazione tra i soggetti privati e la P.A., in quanto tale sistema di comunicazione viene attuato mediante l'utilizzo di un sistema basato su linee di trasmissione di dati ed apparecchiature che consentono di poter documentare sia la partenza del messaggio dall'apparato trasmittente che, attraverso il cosiddetto rapporto di trasmissione, la ricezione del medesimo in quello ricevente. Tali modalità, garantite da protocolli universalmente accettati, indubbiamente ne fanno uno strumento idoneo a garantire l'effettività della comunicazione. Il fax deve presumersi giunto

al destinatario quando il rapporto di trasmissione indica che questa è avvenuta regolarmente, senza che colui che ha inviato il messaggio debba fornire alcuna ulteriore prova, spettando semmai al destinarlo l'onere di provare la mancata ricezione del fax a causa di una difetto di funzionamento dell'apparecchio.
"(CONSIGLIO DI STATO, SEZ. V - *sentenza 19 giugno 2009 n. 4032).''Il fax, per le sue modalità di trasmissione, assicurate da protocolli universalmente accettati, costituisce uno strumento idoneo a garantire l'effettività della comunicazione; in tal senso, infatti, si muove la normativa più recente (d.P.R. 28 dicembre 2000, n. 445), che consente un uso generalizzato del fax nel corso dell'istruttoria, sia per la presentazione di istanze e dichiarazioni da parte dei privati (articolo 38, comma 1), che per l'acquisizione d'ufficio da parte dell'amministrazione di certezze giuridiche (articolo 43, comma 3).Il fax deve presumersi giunto al destinatario quando il rapporto di trasmissione indica che questa è avvenuta regolarmente, senza che colui che ha inviato il messaggio debba fornire alcuna ulteriore prova, spettando semmai al destinarlo l'onere di provare la mancata ricezione del fax a causa di una difetto di funzionamento dell'apparecchio''*(CONSIGLIO DI STATO, SEZ. VI - *sentenza 4 giugno 2007 n. 2951) .*

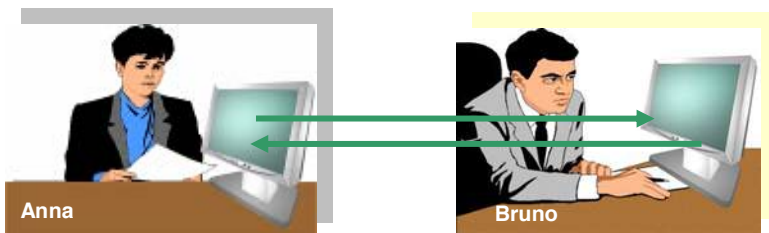
''Il telefax rappresenta uno dei modi in cui possono concretamente attuarsi le comunicazioni tra i privati partecipanti ad un procedimento e la P.A., in quanto tale forma di comunicazione viene attuata mediante l'utilizzo di un sistema basato su linee di trasmissione di dati ed apparecchiature che consentono di poter documentare sia la partenza del messaggio dall'apparato trasmittente che (attraverso il cosiddetto rapporto di trasmissione) la ricezione del medesimo in quello ricevente. Tali modalità, garantite da protocolli universalmente accettati, indubbiamente fanno del telefax uno strumento idoneo a garantire l'effettività della comunicazione. Poiché gli accorgimenti tecnici che caratterizzano il sistema di trasmissione dei documenti mediante telefax garantiscono, in via generale, una sufficiente certezza circa la ricezione del messaggio, ne consegue non solo l'idoneità del mezzo a far decorrere termini perentori, ma anche che un telefax deve presumersi giunto al destinatario quando il rapporto di trasmissione indica che questa è avvenuta regolarmente, senza che colui che ha inviato il messaggio debba fornire alcuna ulteriore prova. Semmai la prova contraria può solo concernere la funzionalità dell'apparecchio ricevente; ma questa non può che essere fornita da chi afferma la mancata ricezione del messaggio'' (CONSIGLIO DI STATO, SEZ. V – *Sentenza 24 aprile 2002 n. 2207).*

Non si vedrebbe quindi l'esigenza di fare una cosa nuova come la PEC-CEC-PAC viste le chiare definizioni delle sentenze.

LA SICUREZZA NELLE E-MAIL (IN PRATICA)

E' indubbio che la corrispondenza ed i documenti di proprietà vadano protetti, perché non siano alla portata di occhi indiscreti e per un'infinità di ragioni logiche. Questo concetto, pur essendo consolidato ed acquisito da ognuno, non viene usato al momento in cui ci si serve di un sistema diverso da quello cartaceo e si perde di vista la sicurezza. E' un fenomeno strano che non si riesce a capire: molti studiosi si sono dedicati a questa casistica. E' il nostro subconscio, che per una sorta di meccanismo, ci convince che tutto quello che facciamo dietro al nostro PC sia inattaccabile e visibile solo a noi, nulla di più sbagliato. La posta elettronica, è uno di quei sistemi, che se non sono usati in modo corretto, possono avere effetti catastrofici soprattutto se i contenuti delle nostre e-mail finiscono nelle mani di malintenzionati . E' bene considerare alcuni sistemi attualmente in uso nel mondo che garantiscono i tre pilastri fondamentali nell'uso delle e-mail:

- **Sicurezza nella trasmissione dei messaggi e loro allegati**
- **Inviolabilità degli stessi**
- **"Non ripudio" nella ricezione degli stessi**

A questo punto sarebbe importante identificare il mezzo che dal 2009 è stato adottato in Italia come strumento primario di comunicazione: la PEC (Posta Elettronica Certificata di cui in appendice si troverà tutta la legislazione):

La PEC (Posta Elettronica Certificata):made in Italy. Così come legiferata ed attuata in Italia:

- Ha bisogno che entrambi i soggetti (Anna e Bruno) abbiano una casella PEC con apparati specifici (es. smartcard);
- Non è interoperabile con altri sistemi, con la produzione dello stesso effetto legale;
- Si perde l'identità della propria e-mail che non potrà più essere quella originale ma dovrà assumere la desinenza del provider PEC (es. @poste.it);
- Non può essere usata per corrispondere con altri paesi;
- Non può essere usata da più postazioni di lavoro, senza una nuova istallazione;
- Non garantisce il "non ripudio" dei contenuti del messaggio e neanche cosa ci sia nel contenuto dello stesso;
- Non ha nessuna portabilità;
- E' complessa nell'istallazione e nella gestione;
- Non permette l'invio di allegati di grandi dimensioni.

È, per ora, relegata solo all'uso con la pubblica amministrazione, dove non ha una grande diffusione.
E'costosa da acquistare e da amministrare. In sostanza non si capisce perché ci sia voluta una legge apposita per la PEC, quando era sufficiente e più semplice l'uso del protocollo S/MIME[62]. Sembrerebbe quasi, che il legislatore ed il relativo "controllore" abbiano creato una forma di ***involuzione del francobollo***, che ormai da oltre un secolo consente di inviare e ricevere corrispondenza in tutto il mondo, senza nessun particolare accorgimento, ma solo in virtù della interoperabilità dei servizi postali, con la conseguenza che all'incremento delle nuove tecnologie corrisponde un decremento della compatibilità. Del resto il solo paese al mondo che ha elaborato una legge apposita per la PEC è l'Italia.

Copre solo i seguenti campi:
Invio/Ricezione certificata di una busta elettronica (busta di trasporto) senza certificazione del contenuto della stessa.

[62] http://www.tech-faq.com/lang/it/s-mime.shtml

EVOLUZIONE LEGISLATIVA DELLA PEC E RELATIVI COMMENTI DI ORDINE TECNICO

La recente legge 28 gennaio 2009, n. 2 art. 6[63] cambia completamente lo scenario della Posta Elettronica Certificata ponendo un'alternativa alla PEC, così come sopra descritta, difatti lo stesso recita "***"o analogo indirizzo di posta elettronica basato su tecnologie che certifichino data e ora dell'invio e della ricezione delle comunicazioni e l'integrità' del contenuto delle stesse, garantendo l'interoperabilità' con analoghi sistemi internazionali***."

In sostanza ognuno può scegliere il sistema di posta elettronica che vuole a condizione che vi sia:

1. L'uso di tecnologie che certificano la data e l'ora dell'invio e della ricezione delle comunicazioni;
2. L'integrità del contenuto delle stesse;
3. La garanzia di interoperabilità con analoghi sistemi internazionali.

Questi tre importanti liberi principi consentono di scegliere un'ampia gamma di provider e soluzioni disponibili a tutti, ma soprattutto garantisce la possibilità di comunicazione con tutto il mondo, a differenza del sistema PEC adottato in Italia, che come più volte ripetuto ha un ambito operativo e legale limitato al solo territorio nazionale.

Questo sistema relega l'Italia all'uso di un sistema inventato solo in questo paese, come si è scritto ampiamente in merito, una per tutte: wikipedia ndr "*E' bene però ricordare che si tratta di uno standard solamente italiano e per adesso nessun altro paese nel mondo ha sentito l'esigenza di crearne uno equivalente. Tecniche di firma digitale[64] e di tracciamento della consegna equivalenti e gratuite sono già disponibili per le e-mail tradizionali da diversi anni.*"

Si affronta finalmente al punto 2), l'integrità del contenuto delle e-mail ed ovviamente dei relativi allegati. La PEC non affrontava il problema e si preoccupava solo del trasporto e dell'integrità della

[63] https://www.globaltrust.it/documents/legaldoc/italia/firma_digitale/28_01_2009.pdf
[64] ht tp://it.wikipedia.org/wiki/Firma_digitale

busta, senza pensare che la stessa, come per le raccomandate A/R, poteva contenere anche un foglio vuoto .

Ma è al punto 3) che si fa il passo più rilevante, infatti in un mondo sempre più globale, mai come ora l'Italia ha bisogno di comunicare con certezze in campo internazionale, esistono da oltre un decennio, previste fra l'altro anche dalla legge Bassanini (l'Italia era tra i primi in Europa nel lontano 1997), sistemi e protocolli sicuri, usati in tutto il mondo, sistemi in cui transitano miliardi di messaggi al minuto.

MA COSA È? COME FUNZIONA LA PEC E I SUOI DERIVATI CEC E PAC?

Molto si è scritto su questa rivoluzione italiana della Posta Elettronica Certificata. E' necessario farne un quadro quanto mai essenziale ed obbiettivo, ma soprattutto indicare le proprietà ed i peccati originali di questo discusso sistema.
La PEC è uno strumento di comunicazione interessante, che nelle intenzioni del legislatore avrebbe dovuto costituire - nelle sue varie applicazioni previste dal nostro ordinamento - uno dei pilastri sui quali fondare la "rivoluzione digitale" nel nostro paese. Tuttavia, la PEC, sin dal suo nascere, è stata caratterizzata da continui interventi normativi, non sempre omogenei e coordinati, tanto da rendere necessario "fare il punto", tecnico e normativo, di tale mezzo di comunicazione, che in sé, contiene la semplicità e la velocità della posta elettronica ordinaria, alle quali aggiunge le caratteristiche di tracciabilità, certificabilità e integrità della comunicazione.

L'origine

Come detto più volte nessun paese al mondo ha sentito il bisogno di creare una "cosa" come la PEC made in Italy essa trae origine dall'emanazione dell'art. 15, comma 2, della legge 15 marzo 1997, n. 59 che definiva il documento informatico, dando un indirizzo normativo basilare allo stesso. Successivamente sono state emanate una serie di leggi, norme, circolari, consolidate nel CAD (Codice dell'Amministrazione Digitale), nella legge istitutiva della PEC e nel suo regolamento (DPR 11 febbraio 2005, n. 68[65])che hanno reso impossibile il funzionamento della stessa con i sistemi di posta elettronica nel resto del mondo. La prima parte del testo normativo è

[65] http://www.cnipa.gov.it/site/_files/DPR%2011%20febbraio%202005%20n.68.pdf

dedicata alla trattazione del diritto dei cittadini e delle imprese, all'uso delle tecnologie telematiche nelle comunicazioni con le pubbliche amministrazioni centrali e con i gestori di pubblici servizi statali in modo programmatico, dispone al Capo IV, dedicato agli strumenti di trasmissione del documento informatico, che gli interessati debbano avere la possibilità di esercitare la partecipazione procedimentale ed il diritto di accesso per mezzo degli strumenti informatici e che lo Stato debba favorire ogni forma di uso delle nuove tecnologie per garantire una maggiore partecipazione dei cittadini al processo democratico.
L'informatizzazione dell'attività amministrativa, se da un lato doveva produrre la dematerializzazione della documentazione, dall'altro lato, ai fini dello svolgimento dell'attività amministrativa digitalizzata, avrebbe dovuto dar vita alla sola circolazione telematica degli stessi.
La circolazione telematica della documentazione amministrativa dematerializzata riguarda i profili della dinamica documentale, che consiste: nella trasmissione telematica della documentazione dai privati, siano essi cittadini o imprese, alle amministrazioni pubbliche; oppure nella trasmissione dei documenti dalle amministrazioni ai privati; o ancora, nella circolazione della documentazione amministrativa tra le amministrazioni pubbliche ordinate allo svolgimento di procedimenti e di attività amministrative.
Nell'ambito della dinamica documentale, assume rilevanza strategica la disciplina della Posta Elettronica Certificata, intesa come strumento di circolazione telematica della documentazione amministrativa tra le amministrazioni pubbliche e tra queste, i privati, le imprese caratterizzata da requisiti rafforzati di certezza, in particolare, la certificazione della spedizione e del ricevimento della comunicazione, ovvero della notificazione di documenti per mezzo posta. Inoltre, lo strumento di Posta Elettronica Certificata rientra tra gli strumenti, descritti dal Codice, idonei per la comunicazione che richiedono la forma scritta e dell'identificazione della fonte di provenienza come requisito di validità.
Prima dell'intervento del legislatore, il mezzo di comunicazione più diffuso per la sua economicità e l'immediatezza di trasmissione era la semplice e-mail, la quale presentava dei punti deboli, quali, ad esempio, la possibilità di falsificare il mittente o l'orario di invio; queste sono state le ragioni che hanno indotto a ricercare forme di comuni-

cazione più sicura, quale la Posta Elettronica Certificata (PEC), nata per assicurare agli utenti la certezza, il valore legale, l'invio e la consegna dei messaggi e-mail al destinatario.
In definitiva la PEC, altro non è, che un sistema di posta, caratterizzata da proprie regole tecniche e giuridiche, la quale fornisce al mittente documentazione elettronica attestante, con pieno valore legale, l'invio e la consegna dei messaggi e-mail; per cui l'ordinaria posta elettronica diventa posta certificata paragonata ad una raccomandata con avviso di ricevimento. L'istituto della PEC trova una sua esplicita regolamentazione non solo negli articoli del Codice dell'Amministrazione Digitale, dedicati espressamente a tale istituto, ma lo scenario normativo è stato ulteriormente arricchito con il D.P.R. 68/2005 "Regolamento recante disposizioni per l'utilizzo della Posta Elettronica Certificata" entrato in vigore il 13 maggio 2005.
Prima di parlare e di esaminare il meccanismo di funzionamento della PEC, con i suoi relativi vantaggi e svantaggi, è opportuno soffermarsi ad analizzare gli "strumenti tecnici" che hanno consentito alla nascita e al relativo sviluppo di questo meccanismo, quali ad esempio: il documento informatico, oggetto di trasmissione per via telematica; la firma digitale e il relativo valore probatorio del documento firmato con tale supporto tecnologico.
Questa spinta doveva essere di indirizzo e non di regole giuridiche e legali molto specifiche in una materia così complessa, come affermato da un autorevole giurista Franco Bassanini nel convegno a dieci anni dalla legge che porta il suo nome[66].
La tecnologia è in continua evoluzione *"ma le leggi non sono in grado di correre come la tecnologia"* conseguentemente viene emesso il semplice teorema contenuto nella stessa legge Bassanini Legge 15 marzo 1997, n. 59 art 15/2 *"Gli atti, dati e documenti formati dalla pubblica amministrazione e dai privati con strumenti informatici o telematici, i contratti stipulati nelle medesime forme, nonché la loro archiviazione e trasmissione con strumenti informatici, sono validi e rilevanti a tutti gli effetti di legge*", dopo questa chiara enunciazione sono state aggiunte una ridda di norme che per essere rappresentate hanno bisogno di un grafico (figura in basso).

[66] https://www.cybercrimeworkinggroup.org/Default.aspx?tabid=145

A queste si sono aggiunte le ultime normative del 2009 contenute, fra l'altro, in provvedimenti detti *"omnibus"*, che di tutto trattano fuorché della materia specifica, oltre ad una completa riforma del CAD Codice dell'amministrazione digitale appena approvato D.L. 30/1272010 n°235, che ho riportato in appendice.

Schema di funzionamento della Posta Elettronica Certificata

Posta elettronica certificata
- schema funzionale -

Dominio di posta certificata mittente

Dominio di posta certificata destinatario

1 - Composizione messaggio, collegamento al gestore

2 - identificazione utente, controlli di sicurezza e formali

3 - invio ricevuta di accettazione

4 - imbustamento e trasmissione

5 - controlli di provenienza, integrità, formali e di sicurezza

6 - invio ricevuta di presa in carico al gestore del mittente

7 - Consegna nella casella postale (indirizzo telematico) del destinatario

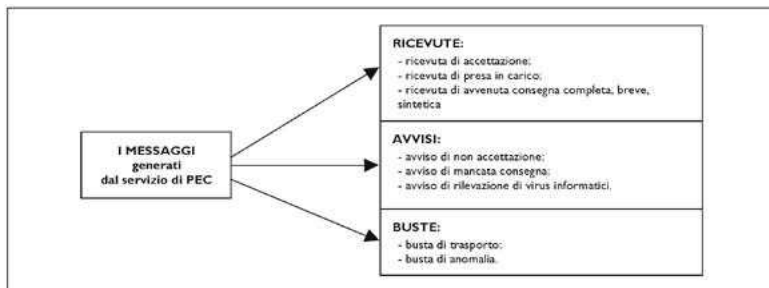
8 - invio ricevuta di consegna al mittente

9 - lettura messaggio

Dovendo operare in un contesto dove gli standard sono indispensabili, la PEC come base non si differenzia dal normale funzionamento delle e-mail, altrimenti non funzionerebbe. Intorno agli standard sono state apportate delle modifiche sostanziali cercando di rendere sempre più vicina l'e-mail alla raccomandata con ricevuta di ritorno. Particolare attenzione è stata posta sulla gestione delle ricevute di ritorno, piuttosto che sull'integrità del contenuto dei messaggi, usando in modo anomalo le disposizioni relative alla firma digitale, da parte dei gestori come, disposto dell'art. 1, D.P.R. del n. 445/2000; al fine di ricavare un'indicazione temporale di riferimento opponibile a terzi con l'uso della *"busta di trasporto"* come sistema di trasmissione e firma digitale, ampiamente descritto nel DPR 11 febbraio 2005, n.68. Questo è stato un vero e proprio cavallo di battaglia da parte degli inventori di questo sistema, se non la base stessa del "teorema Italico" della Posta Elettronica Certificata, in cui la più volte richiamata ***"busta di trasporto"*** fa la parte del leone nella gestione di un messaggio di posta elettronica e non i contenuti della stessa, che dovrebbero essere primari rispetto alla busta. Una serie di importanti rilievi fatti da giuristi e tecnici[67] portano il legislatore a

[67] http://www.altalex.com/index.php?idnot=49104

sfornare un nuovo dispositivo di legge D.P.C.M. 6 maggio 2009[68] sul rilascio e uso della casella di PEC ai cittadini. Si specifica che: *"Le pubbliche amministrazioni accettano le istanze dei cittadini inviate tramite PEC nel rispetto dell'art. 65, comma 1, lettera c), del decreto legislativo n. 82/2005[69]. L'invio tramite PEC costituisce sottoscrizione elettronica ai sensi dell'art. 21, comma 1, del decreto legislativo n. 82/2005[70];"* Equiparando così, con un tratto di penna, la firma digitale di un documento alla PEC, dandole la stessa valenza giuridica ed annullando *"defacto"* buona parte del CAD in materia.

Il documento informatico trasmesso per via telematica si intende spedito dal mittente, se inviato al proprio gestore, e si intende consegnato al destinatario, se reso disponibile nella casella di Posta Elettronica Certificata contraddistinta dal relativo indirizzo elettronico da questi dichiarato nella casella di posta elettronica certificata del destinatario, "affittata" dal gestore a quest'ultimo.
I sistemi di gestione della PEC, durante i passaggi intermedi dal mittente al destinatario finale, anche nel caso in cui il mittente ed il destinatario appartengano allo stesso dominio di Posta Elettronica Certificata, generano dei messaggi specifici (come detto, per funzionare debbono essere conformi allo standard internazionale S/MIME) elaborati in base alla tipologia di messaggio e distinti in tre categorie: le ricevute, gli avvisi e le buste (vedi figura in basso).

Con la certificazione delle fasi del servizio di PEC, il mittente riceve dal gestore della Posta Elettronica Certificata una ricevuta, che costi-

[68] http://www.altalex.com/index.php?idnot=46242
[69] http://www.altalex.com/index.php?idnot=9618
[70] http://www.altalex.com/index.php?idnot=9618

tuisce prova legale dell'avvenuta spedizione della "busta di trasporto" contenente il messaggio e l'eventuale documentazione allegata che rimane sconosciuta al destinatario fino all'apertura della cosiddetta "busta di trasporto".
Stessa cosa avviene nell'ufficio postale che accetta una busta chiusa, assimilabile alla busta di trasporto della PEC, che attesta con vari timbri e ricevute l'accettazione della stessa e s'impegna a consegnarla al destinatario con la procedura della raccomandata con ricevuta di ritorno. Anche se in modo più blando, l'ufficio postale s'impegna altresì, a restituire al mittente la ricevuta di ritorno (che viaggia con posta ordinaria), oppure in caso di mancato ricevimento, restituisce il plico integro al mittente, nei tempi stabiliti dal regolamento postale, con le motivazioni della mancata consegna. In nessuno dei due casi, PEC e Posta Raccomandata con ricevuta di ritorno, il gestore entra nel merito del contenuto della Raccomandata AR o della "busta di trasporto PEC". Ai fini della validità della trasmissione e della ricezione della "busta di trasporto" contenente il messaggio di Posta Elettronica Certificata ed eventuali allegati vengono rilasciate, rispettivamente:

1. ricevuta di accettazione, proveniente dal proprio gestore di posta, che attesta l'avvenuto invio della "busta di trasporto" contenente il messaggio e-mail ed eventuali allegati;
2. ricevuta di presa in carico, che attesta il passaggio di responsabilità dall'utente al gestore;
3. ricevuta di avvenuta consegna nelle varie forme completa, breve, sintetica, proveniente dal gestore di posta del destinatario, che certifica che quest'ultimo abbia ricevuto la comunicazione. Tale certificazione sarà resa nel momento in cui il destinatario avrà disponibilità del messaggio (ossia al momento del ricevimento), indipendentemente dal fatto che egli lo abbia aperto, letto o meno.

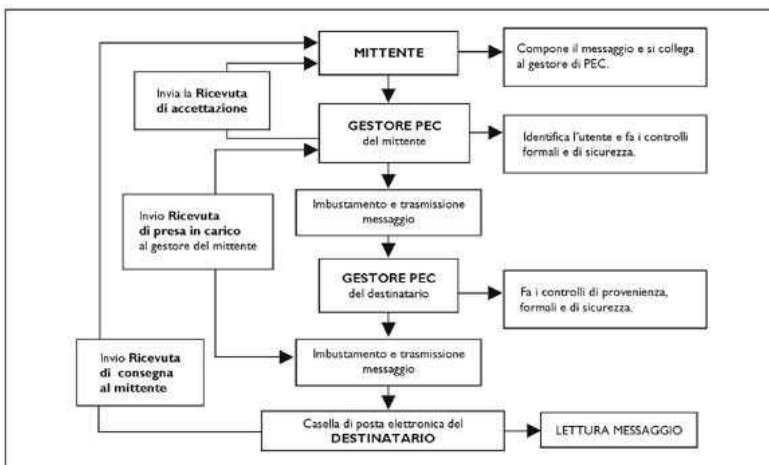
Il meccanismo con il quale il sistema funziona, è quello della certificazione con firma digitale X.509 della sola "*busta di trasporto",* così come specificato dal DPR 11 febbraio 2005, n.68 che regola anche gli avvisi generati dal sistema di Posta Elettronica Certificata che possono essere:

a) avviso di non accettazione (per eccezioni formali o virus informatici);

b) avviso di mancata consegna (per il superamento dei tempi massimi previsti o per virus informatici); in caso di un'eventuale mancata ricezione da parte del destinatario cioè il server del gestore, il gestore di posta di quest'ultimo, informerà il mittente, qualora entro 24 ore non sarà riuscito ad effettuare la consegna del messaggio;
c) avviso di rilevazione di virus informatici.

Le tipologie di buste create dal sistema possono essere:

a) busta di trasporto (contenente il messaggio originario, i dati di certificazione e la firma del gestore sulla relativa "busta di trasporto");
b) busta di anomalia (contenente varie anomalie per cui "la busta di trasporto" e i suoi contenuti non possono essere trattati).

Tutte le tipologie, dei messaggi generati dal sistema PEC, sono sottoscritti dai gestori di Posta Elettronica Certificata mediante la firma digitale applicata alla "busta di trasporto". I certificati di firma, di cui il gestore deve disporre ai fini della validità della certificazione del messaggio, sono rilasciati dal CNIPA al momento dell'iscrizione nell'elenco pubblico dei gestori di Posta Elettronica Certificata e sino ad un numero massimo di dieci firme per ciascun gestore (ai sensi dell'art. 7 del D.P.C.M. 2 novembre 2005 è prevista la possibilità di richiedere un numero di certificati di firma superiore a 10 da parte dei gestori). Il percorso dal mittente, al destinatario finale del messaggio di PEC è di seguito schematizzato attraverso una sequenza che illustra le fasi del passaggio, dal mittente al rispettivo gestore e dal gestore del destinatario al destinatario stesso, evidenziando i momenti in cui il servizio di PEC genera le tre tipologie di ricevute descritte in precedenza (vedi figura).

E' il caso di fare particolare attenzione a questa pratica della firma digitale apposta sulla "busta di trasporto", secondo la normativa, al fine di salvaguardare le due parti, mittente e destinatario, e dare sicurezza a quanto contenuto nella"busta di trasporto".
Tutto il meccanismo della PEC-CEC-PAC si incentra sulla **"Busta di Trasporto"**regolata sia dal **D.P.R. n. 68/2005**[71], che dal ***DECRETO 2 novembre 2005***[72]: "*Regole tecniche per la formazione, la trasmissione e la validazione, anche temporale, della Posta Elettronica Certificata*".
Difatti, il messaggio che noi prepariamo, viene imbustato nella cosiddetta "busta di trasporto" dal gestore del mittente e spedita al gestore del destinatario, ed è bene fare particolare attenzione a questo nuovo sistema dove la firma digitale viene apposta sulla "busta di trasporto" secondo la normativa, al fine di salvaguardare le due parti mittente e destinatario e dare sicurezza a quanto contenuto nella "busta di trasporto".
Orbene, con questa procedura si modifica la natura della firma digitale ed i suoi scopi, infatti è nata, non solo per certificare colui che firma un documento, oggi anche i contratti ed altri atti amministrativi, ma per sostituire la firma autografa, normalmente autenticata da un notaio o da un pubblico ufficiale. Accomunandola al timbro che l'ufficio postale appone al plico raccomandato, forse la firma digitale non è usata nel modo più proprio, con un'importante aggravante di

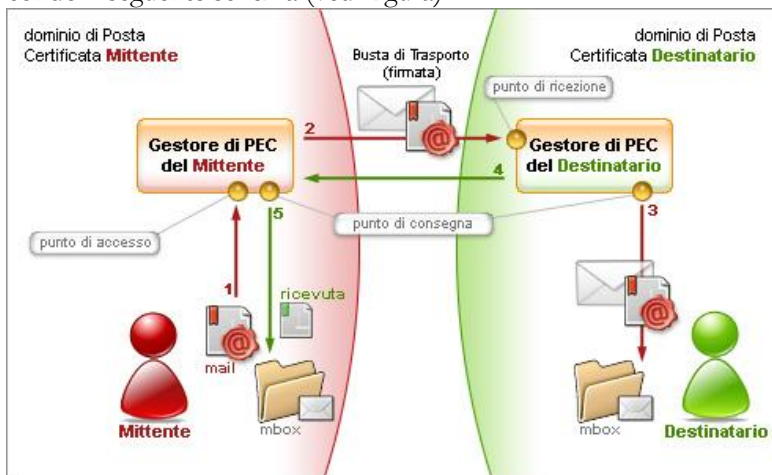
[71] http://www.cnipa.gov.it/site/_files/DPR%2011%20febbraio%202005%20n.68.pdf
[72] http://www.cnipa.gov.it/site/_files/DECRETO%202%20novembre%202005.pdf

ordine tecnico, che approfondisco, ma anche di tipo giuridico, che lascio ai giuristi:

1. La firma digitale è univoca ed appartiene per la sua natura alla persona fisica che l'ha richiesta, nel rispetto delle procedure stabilite dalla legge istitutiva della stessa, nonché delle direttive comunitarie relative (la prima fu la "93/99)[73];
2. Il titolare della firma digitale è soggetto ad una serie di cautele sull'uso, la conservazione e la messa in sicurezza della stessa, conservazione in apparati sicuri, uso avanzato di password ecc. per impedirne un uso improprio;
3. L'uso è ristretto alla firma di documenti in forma digitale, la formazione dei quali, ha valenza giuridica e tale concetto è riportato nella legge Bassanini all'art. 15/2 in modo piuttosto chiaro: *"Gli atti, dati e documenti formati dalla pubblica amministrazione e dai privati con strumenti informatici o telematici, i contratti stipulati nelle medesime forme, nonché la loro archiviazione e trasmissione con strumenti informatici, sono validi e rilevanti a tutti gli effetti di legge*";
4. Il principio su enunciato, cardine di tutte le norme successive, non entra minimamente nel merito di come il documento debba essere spedito, archiviato, trattato;
5. Una delle caratteristiche della firma digitale è quella di garantire l'inalterabilità del documento una volta firmato, conseguentemente lo stesso in qualsiasi modo venga spedito, archiviato o altro deve rimanere integro ed originale, può anche essere criptato e/o protetto da password, per non renderlo intellegibile a terzi.

Esaminando invece cosa avviene nel mondo PEC, il gestore, né più né meno come l'ufficiale postale mette un timbro, firma, con un'unica o più firme digitali a sua disposizione, le buste in cui transitano tutti i documenti spediti attraverso la PEC e li conserva nei server di sua proprietà, le cui porzioni sono "affittate" dai titolari di caselle PEC. Scambia le chiavi, costituenti la firma digitale con altri gestori, invia le "buste di trasporto" che contengono i messaggi ed i relativi allegati al gestore del destinatario, generando il traffico come

[73] https://www.globaltrust.it/documents/legaldoc/mondo/europa/1999_93_en.pdf

precedentemente descritto, composto da messaggi e ricevute, secondo il seguente schema (vedi figura)

Come l'addetto alla sicurezza di un albergo accede con il pass partout in qualsiasi camera, il gestore dall'una (mittente) e dall'altra parte (destinatario), ha la possibilità di accedere con le proprie credenziali in qualsiasi casella di Posta Elettronica Certificata (equiparabile alla stanza d'albergo), ed aprire qualsiasi messaggio in essa contenuto in quanto tenutario della chiave crittografica X-509 (firma digitale) di tutte "le buste di trasporto" dei suoi clienti titolari di caselle PEC-CEC-PAC. Questo fatto, tecnicamente incontrovertibile, stravolge tutte le normative anche costituzionali (Art. 15 *La libertà e la segretezza della corrispondenza e di ogni altra forma di comunicazione sono inviolabili.*) sulla protezione della corrispondenza è diverso dalla raccomandata che ritorna integra al mittente in caso di mancata consegna. Entrambi sono soggetti, oltre che a fatti di illegalità, di infedeltà dei dipendenti, del gestore ecc. anche ad intercettazioni, peraltro libere e non soggette all'odierna storia infinita della legge sulle intercettazioni, in discussione da oltre 5 anni che si occupa prevalentemente di fonia (telefonate) da parte dell'Autorità Giudiziaria. Questa infatti, con una semplice ordinanza di poche righe può disporre, ad esempio a Poste Italiane,*"di intercettare tutti i messaggi in arrivo e in partenza dalla casella PEC del Sig. Rossi e richiederne una copia"*. Sistema semplice e rapido per avere tutto, *ma proprio tutto*, già trascritto e pronto all'uso.

Mi sembra quindi sostanziale la differenza con un sistema S/MIME dove il messaggio transita:

1) Attraverso un provider di nostra fiducia e non imposto da nessuno;
2) Può essere criptato e conseguentemente, anche se intercettato da un malintenzionato o dall'autorità, non può essere utilizzato;
3) In sostanza ha le stesse caratteristiche della PEC-CEC-PAC, con in più la riservatezza, oltre la firma digitale sul documento e non a protezione della busta di trasporto;
4) Può essere usato in tutto il mondo. E non si può dire che non se ne sia discusso, Cittadini di Internet, nel 2009 ad esempio, organizzò un convegno a Roma dal titolo significativo: *"Privacy ed Intercettazioni, non solo telefonate"*[74].

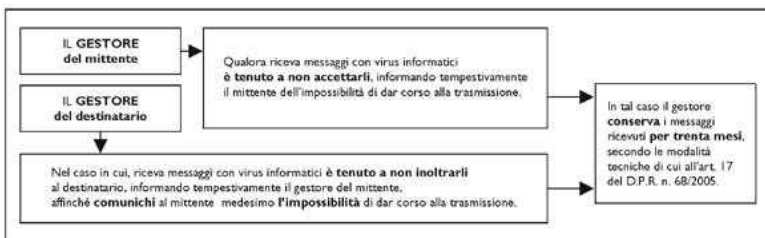
In caso di un'eventuale mancata ricezione da parte del destinatario il gestore di posta dello stesso, informerà il mittente qualora entro 24 ore non sia riuscito ad effettuare la consegna della "busta di trasporto" contenente il messaggio.

I gestori sono tenuti (non obbligati) a verificare che il messaggio di posta elettronica non sia contagiato da virus e ad adottare i comportamenti disciplinati all'art. 12 del D.P.R. 68/2005 (vedi figura).

Il D.P.R. n. 68/2005 stabilisce anche una soluzione per l'eventuale smarrimento delle ricevute; infatti, un apposito archivio informatico custodito dai gestori di Posta Elettronica Certificata ha il compito di conservare, per un periodo di trenta mesi, le tracce informatiche caratterizzate dallo stesso valore giuridico.

Quello che non si riesce a capire è, come tecnicamente si riescano a separare le ricevute dai contenuti, che formano l'intero messaggio in un'e-mail e viaggiano in modo inscindibile.

E' evidente, che i gestori conservano l'intero messaggio nella casella di PEC-CEC-PAC, anche se contenuto nella "busta di trasporto" firmata digitalmente, di cui il gestore conserva le credenziali e le chiavi per aprirla ad ogni legittima richiesta, oltre a correre il rischio di essere aperta da intrusi che sono o possono entrare in possesso delle chiavi di accesso.

[74] *Il post evento filmati ed interventi dei relatori* https://www.convegnieventi.com/pagina.asp?id=13

Infine, con il decreto 2 novembre 2005: *"Regole tecniche per la formazione, la trasmissione e la validazione, anche temporale, della Posta Elettronica Certificata"*, si è voluto dare un impianto tecnico alla PEC.
Se si scorrono le stesse regole, si vedrà che la base è data da protocolli standard ampiamente descritti in questo libro, con la costruzione sopra agli standard stessi di comunicazione, di una serie di accorgimenti che rendono la PEC non interoperabile con nessun sistema di Posta Elettronica Certificata e non in uso in tutto il mondo.
Rimane l'interrogativo: Allora perché usare questo sistema?

I difetti della PEC

Qui di seguito si elencano i principali difetti della PEC come inserite nel nostro ordinamento da me definiti i ***"peccati originali della PEC":***

- Essere stata concepita e fatta nascere ed ora, costretta a crescere come imposizione dall'alto, tramite leggi, decreti, norme e bandi di gara, senza preoccuparsi di creare un adeguato contesto;
- Voler creare per forza uno strumento simile in tutto e per tutto alla raccomandata con ricevuta di ritorno, in un ambiente diverso (digitale/informatico) da quello fisico;
- Ignorare l'evolversi delle tecnologie, determinando delle regole tecniche, pensate anni prima ed attuate anni dopo, su protocolli universalmente riconosciuti e funzionanti con tutta una serie di aggiunte e varianti inutili, limitate al contesto territoriale italiano ed inesistenti nel resto del mondo;
- Voler creare la figura del gestore di PEC, una sorta di "notaio ibrido" non conforme al nostro ordinamento di base;
- Voler dare al gestore incombenze (ora e data) dei messaggi, già risolte universalmente dalle stesse tecnologie, che non hanno bisogno, per la loro natura, di certificazioni di terze parti;

- Istituire, in modo a dir poco sibillino, una "residenza/domicilio virtuale/elettronico" di cittadini professionisti ed imprese, unico al Mondo;
- Costruire una casella di posta (PEC), ora chiamata fascicolo informatico, impossibile da gestire special modo dal lato PA, con un aggravio di spesa lato impresa e PA;
- Non aver reso pubblico, se mai ne esista uno, un adeguato studio di fattibilità della PA in materia di PEC e di impatto per il sistema impresa/professionisti e per tutti noi;
- Non aver mai pensato di adottare un sistema interoperabile con altri sistemi Internazionali ed averlo inserito con un articolo di legge, teorico, ma non ancora reso operativo dopo 5 anni dall'emanazione della legge sulla PEC, precisamente l'Art.16/6 legge n° 2 gennaio 2009 che recita ***o analogo indirizzo di posta elettronica basato su tecnologie che certifichino data e ora dell'invio e della ricezione delle comunicazioni e l'integrità del contenuto delle stesse, garantendo l'interoperabilita' con analoghi sistemi internazionali."*** Rinviato ad un regolamento tecnico dove risulta evidente che è la PEC a dover divenire interoperabile con Gli analoghi sistemi Internazionali Art.35 LEGGE 18 giugno 2009 , n. 69 " *1. Entro sei mesi dalla data di entrata in vigore della presente legge, il Governo adotta, ai sensi dell'articolo 17, comma 1, della legge 23 agosto 1988, n. 400, e successive modificazioni, un regolamento recante modifiche al regolamento di cui al decreto del Presidente della Repubblica 11 febbraio 2005, n. 68, anche al fine di garantire l'interoperabilità del sistema di posta elettronica certificata con analoghi sistemi internazionali."*
- Aver immaginato un sistema, in cui si da solo rilevanza alla "busta di Trasporto", invece che ai contenuti del messaggio e suoi allegati;
- Determinare, con regole tecniche studiate ad hoc, il ricevimento virtuale di PEC in apparati SERVER di terze parti (gestori), dai quale vengono a generarsi tempi, scadenze, prescrizioni e sanzioni a prescindere dall'effettiva recezione o meno del Messaggio di PEC da parte del soggetto interessato;
- Aver ingenerato l'illusione, che il cosiddetto gestore, è il conservatore solo dei "Log dei messaggi" e non dell'intero messaggio ed allegati relativi, cosa tecnicamente impossibile e

smentita poi dalla "creazione del "fascicolo elettronico", che altro non è che la casella di PEC con l'intero suo contenuto di documenti e messaggi che transitano nel sistema;

- Aver ingenerato una confusione legislativa con l'accavallarsi di norme che dal 1997 hanno raggiunto una mole allucinante;
- Aver usato termini e nomenclature tecniche, non solo incomprensibili, ma contrastanti tra loro. Un esempio per tutti: pochi hanno capito se la PEC è una casella di Posta elettronica od un indirizzo di posta elettronica! Due cose ben diverse, ma usate qua e là nelle disposizioni di legge, senza logica ed ordine;
- Non aver prima dotato e rese operanti normative che risalgono al CAD (Codice della Amministrazione Digitale), anziché far operare prima la PA attraverso la PEC rendendola disponibile poi ai cittadini.

Solo con l'Art. 34 LEGGE n.° 69 del 16 Giugno 2009, giunto ben quattro anni dopo l'emanazione del CAD, si obbliga la PA ad inserire nella Home Page (pagina iniziale) dei siti WEB un indirizzo PEC entro il 30 Giugno 2009, cioè 6 mesi dopo l'emanazione della legge !!?? Norma questa de facto disattesa da buona parte della Pubblica Amministrazione centrale e periferica.

IL CERTIFICATO DI FIRMA, LA POSTA ELETTRONICA E IL PROTOCOLLO S/MIME

Con il protocollo S/MIME:

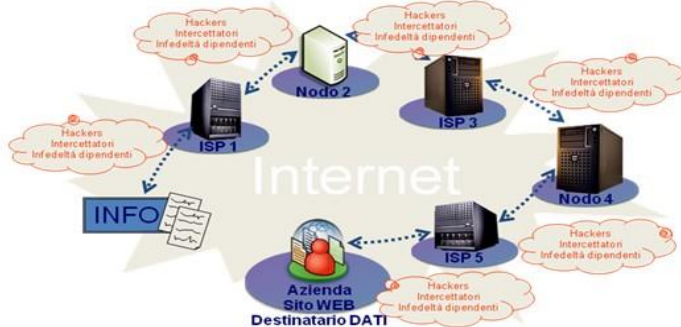
- Anna e Bruno non hanno bisogno di nessun apparato specifico, a meno che lo vogliano. In tal caso possono scegliere qualsiasi cosa: token, usb, floppy, ecc.;
- Il protocollo è interoperabile con qualsiasi sistema;
- E' valido in tutto il mondo;
- Esportando od istallando più certificati può essere usato su più postazioni;
- La perdita di un certificato non comporta nessuna prassi burocratica (denuncia di smarrimento od altro) è sufficiente chiederne la revoca e non avrà più alcun valore, né potrà essere usato da nessuno;

- Garantisce il "non ripudio" del messaggio e dei contenuti dello stesso e relativi allegati
- Con funzioni di Time Stamping, qualora implementate dal sistema, garantisce e rende legali l'ora e la ricezione del messaggio;
- Ha la massima portabilità e si può utilizzare, con la combinazione di sistemi come *"Certified-Mail"*, da qualsiasi postazione che abbia una connessione Internet per l'inoltro di allegati voluminosi;
- E' semplice da gestire e da installare;
- Permette, ad esempio con Certified-Mail[75], di inviare allegati fino a 4GB;
- È usufruibile da tutti ed ha valenza anche nei confronti della pubblica amministrazione;
- E' molto economico da amministrare ed acquistare;
- Ampie applicazioni e flessibilità, l'esempio Blackberry[76]

Contrariamente a quanto si pensa, la trasmissione dei dati non avviene direttamente tra due soli soggetti, ma è facilmente intercettabile (vedi figura)

75 http://www.certifiedmail.it/
76 http://www.blackberry.com/it/products/enterprisesolution/security/smime.shtml

L'inizio del Problema

La trasmissione dei dati, dopo aver premuto il tasto **INVIA** o **CONFERMA**, è **incontrollata** ed **incontrollabile**. I dati vanno in rete e transitano in un numero imprecisato di **Server/Computer**, linee telefoniche, connessioni, etc. facilmente intercettabili e/o sottraibili in tutto il loro percorso ed archiviazione.

LA MARCA TEMPORALE, TIME STAMP, L'ORIGINALITA' DEL DOCUMENTO

La nuova disposizione di legge, come già detto, ripresenta il problema, non banale, dei contenuti del messaggio di posta, che non è limitato al testo, contenuto, ma anche agli allegati degli stessi, cosa piuttosto comune nella pratica di ogni giorno.

Garantire quindi i contenuti e non la "*busta di trasporto*" è una buona pratica, che risolve non pochi problemi. Indispensabili per questa forma di comunicazione certificata sono:

1. La certificazione con firma digitale;

2. Il documento deve rimanere integro in tutto il percorso fino all'arrivo al destinatario ed alla sua archiviazione;

3. Deve essere garantita la privacy, conseguentemente la Best Practice è quella della criptazione dell'e-mail e dei suoi allegati, che non è proprio un eccesso di prudenza, ma la sicurezza che il messaggio non venga intercettato o aperto da chiunque. Esistono sistemi ancora più sofisticati che prevedono in alcuni casi la distruzione irreversibile dello stesso dopo che è stato letto;

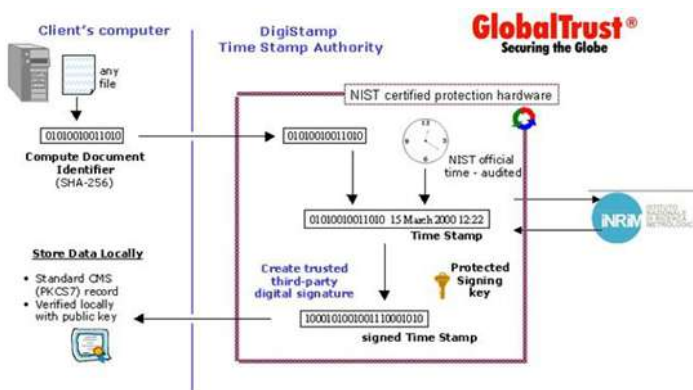
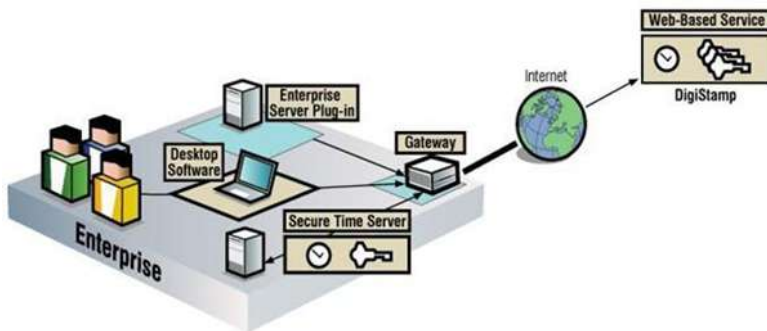
4) Deve essere garantita, qualora sia necessario, la data, ed in alcuni casi anche l'ora certa dell'elaborazione del documento. La PEC prevede solo la data e l'ora certa di spedizione della "busta" che non ha nulla a che vedere con il contenuto della stessa, cioè il documento, quando questo si sia formato e sottoscritto digitalmente ed eventualmente scambiato tra le parti, cioè firmato digitalmente dall'altra parte.
   Il riferimento nella nuova norma al fatto che: "*certifichino data e ora dell'invio e della ricezione delle comunicazioni e l'integrità' del contenuto delle stesse, garantendo l'interoperabilità' con analoghi sistemi internazionali,*" spiega finalmente in modo semplice e conciso cosa si vuole, che poi è il sistema già usato in tutto il mondo.

5) È importante notare l'interesse del legislatore a "*garantire l'interoperabilità con analoghi sistemi internazionali*" attraverso il sistema di marche temporali o TIME STAMP.
   Da tempo, infatti, tutto il sistema degli "orologi" che garantiscono l'ora e la data di comunicazione sono interoperabili in tutto il mondo (del resto diversamente non potrebbe essere) e in tutti i paesi esiste un organismo che regola l'ora interoperabile con tutti gli altri. In Italia http://www.inrim.it/, che è a sua volta collegato a tutti gli altri paesi e per i sistemi informativi (computer) si usa il protocollo NTP Network Time Protocol[77].
   Il tempo coordinato universale[78] (UTC) è la base temporale legale per tutto il mondo e segue il TAI, con uno scarto di un certo numero di secondi[79] (attualmente 34). Tali secondi sono inseriti su consiglio dell'International Earth Rotation and Reference Systems Service[80] (IERS), per fare in modo che, come media sugli anni, il Sole[81] sia al meridiano di Greenwich[82] entro 0,9 secondi dal 12:00:00 UTC.

Tutto questo per far capire quanto sia importante la standardizzazione di tutti i sistemi , dove una data e un'ora devono essere riconosciute da tutti globalmente senza possibilità di dispute di nessun

[77] http://it.wikipedia.org/wiki/Network_Time_Protocol
[78] http://it.wikipedia.org/wiki/Tempo_coordinato_universale
[79] http://it.wikipedia.org/wiki/Secondo
[80] http://it.wikipedia.org/wiki/International_Earth_Rotation_and_Reference_Systems_Service
[81] http://it.wikipedia.org/wiki/Sole
[82] http://it.wikipedia.org/wiki/Meridiano_di_Greenwich

genere ma soprattutto non possono essere regolate da leggi naziona-li.

Qui di seguito alcuni grafici che meglio illustrano il sistema di *time stamping:*

In Italia la data e l'ora vengono ulteriormente sincronizzate attraver-so L'Istituto Nazionale di Ricerca Metrologica (I.N.RI.M).

Avviso da inserire nei messaggi di posta con certificato S/MIME

È consigliabile inserire nei messaggi di posta elettronica un avviso come ad esempio:

"*E-MAIL FIRMATA DIGITALMENTE: questa e-mail, se firmata digitalmente, ha valore legale ai sensi della normativa vigente, maggiori info.*[83]"

Questo servirà a far capire all'interlocutore, che il messaggio che state inviando ha tutte le caratteristiche previste dalle leggi sulla firma digitale in vigore, non solo in Italia, ma anche in molti paesi del mondo e per questo motivo è opportuno inserire un testo anche in lingua inglese come segue:

"***E-MAIL DIGITALLY SIGNED***: *this message is digitally signed and has legal value according to international law and treaties.*"

Entrambi gli avvisi potranno essere linkati verso le maggiori sorgenti di informazione nazionali e internazionali in modo da fornire all'interlocutore un'informazione corretta.
Attenzione agli antivirus gratuiti ed alle firme. Nell'usare antivirus gratuiti può avvenire che questi inseriscano un messaggio pseudo pubblicitario del tipo: *"questo messaggio è stato controllato dall'antivirus x"*. E' la classica violazione in un messaggio firmato digitalmente, anche se le intenzioni sono buone, cioè quelle di avvertire il ricevente che il messaggio è esente da virus, è pur sempre un cambiamento/aggiunta al testo del messaggio scritto. S/MIME farà il suo dovere ed invierà un allert al destinatario avvertendolo che il messaggio è stato alterato durante la trasmissione, ed infatti è il sistema del controllo dei virus nei messaggi in uscita, che avrà inserito la frase e non il mittente. E' buona norma non consentire a nessun sistema automatico o non automatico di inserire qualsiasi cosa dopo che il messaggio è stato firmato digitalmente.

[83] http://www.globaltrust.it/seclaw/index.aspx

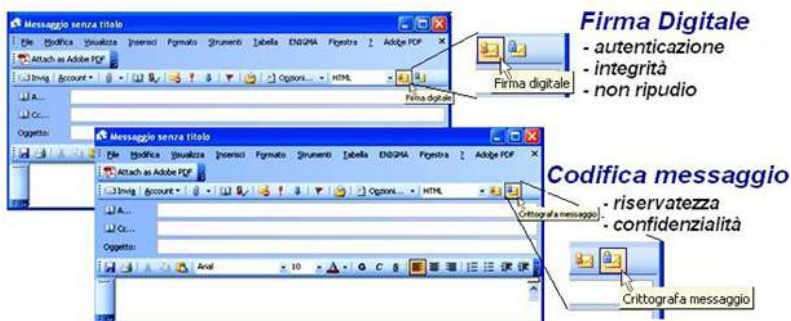
CAPITOLO V. 5.0

INSTALLAZIONE ED USO DEI CERTIFICATI DI FIRMA S/MIME

INTRODUZIONE AI CERTIFICATI S/MIME E ALLA POSTA ELETTRONICA CERTIFICATA FIRMATA DIGITALMENTE

I certificati S/MIME, utilizzati per la Posta Elettronica Certificata, permettono di **firmare e cifrare** digitalmente i messaggi di posta e-lettronica (e-mail) ed eventuali allegati associati, garantendo nello stesso tempo **sicurezza** e **confidenzialità** delle informazioni.

In particolare:

- **codificare** i messaggi di posta elettronica permette di garantire **riservatezza** e **confidenzialità** dei dati inviati in rete utilizzando come strumento la posta elettronica;
- **firmare digitalmente** i messaggi di posta elettronica permette di garantire **autenticità, integrità e "non ripudio"** dei dati inviati in rete utilizzando come strumento la posta elettronica.

Cosa significa integrità dei dati e riservatezza in un'e-mail firmata?

La firma digitale garantisce l'integrità dei dati e permette di verificare se il messaggio che si sta leggendo sia stato alterato, per cause acci-

dentali o intenzionali. La cifratura, invece, assicura la riservatezza e la confidenzialità dei dati inviati in Rete, consentendo solo all'effettivo destinatario di recuperare e leggere il messaggio.

Cosa significa "non ripudio"?

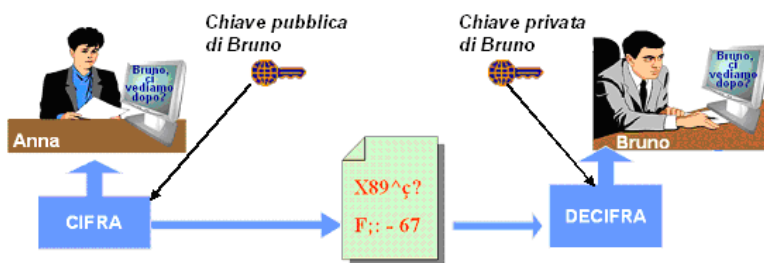
La caratteristica primaria della firma digitale è di permettere all'autore (firmatario) di un messaggio, di provare la sua identità al destinatario apponendovi la propria firma. Il "non ripudio" permette inoltre di provare l'identità di tutte le parti che hanno partecipato ad una transazione (scambio di messaggi di posta elettronica), anche in un momento successivo rispetto a quello in cui si è verificata la transazione l'invio del messaggio Il firmatario di un documento trasmesso non può negare di averlo inviato, né il ricevente negare di averlo ricevuto. Più semplicemente, "non ripudio" significa che l'informazione non può essere disconosciuta, come una firma a mano davanti a testimoni od un notaio su un documento cartaceo.
E' bene sottolineare che la principale differenza tra firma autografa e firma digitale sta nel fatto che la prima, è direttamente riconducibile all'identità di colui che la appone, perché la calligrafia è un elemento identificativo della persona, mentre la seconda non possiede questa proprietà.
Per coprire questa deficienza si ricorre ad un'Autorità di Certificazione (Certification Authority, CA) che ha il compito di stabilire, garantire e pubblicare l'associazione tra un utente e la sua chiave pubblica, attraverso uno strumento denominato "certificato digitale".
Il certificato digitale in sostanza è una sequenza di bit che rappresenta informazioni relative alla persona (nome, cognome, e-mail, ecc.) e le associa ad una chiave pubblica. Due utenti che vogliono comunicare in modo sicuro utilizzando come strumento di protezione il certificato digitale, non fanno altro che scambiarsi la propria chiave pubblica in modo tale da utilizzarla in seguito per decodificare/verificare il messaggio protetto.

Che tipo di chiavi sono utilizzate per le firme digitali

La firma digitale si basa sulla crittografia a chiave asimmetrica (crittografia a chiave pubblica) e utilizza una coppia di chiavi di cui una è resa pubblica. Dalle due chiavi una viene usata per codificare (firmare) e l'altra per decodificare (verificare) un messaggio.

Come viene cifrato il contenuto di un messaggio di posta elettronica

Per cifrare il contenuto di un messaggio di posta elettronica (inclusi eventuali allegati) deve essere utilizzata la chiave pubblica del destinatario del messaggio senza la quale è impossibile leggere lo stesso.

ATTENZIONE: In questo modo <u>solo il destinatario, con la propria chiave privata, è in grado di leggere il contenuto del messaggio.</u>

- **Anna** deve inviare dei dati riservati a Bruno
- **Anna** cifra i dati utilizzando la chiave pubblica di Bruno

- **Bruno** decodifica il messaggio cifrato da Anna, utilizzando la sua chiave privata (chiave segreta, unica chiave in grado di decifrare il messaggio)

Come viene firmato un messaggio di posta elettronica

Per firmare digitalmente un messaggio di posta elettronica deve essere utilizzata la chiave privata del firmatario (mittente). Il destinatario verificherà poi la legittimità della firma, utilizzando la chiave pubblica del mittente.

In breve
Per utilizzare la crittografia, quando si inviano e si ricevono i messaggi di posta elettronica, è innanzitutto necessario un ***ID DIGITALE*** *che può essere richiesto ad un'autorità di certificazione (CA) (es. GlobalTrust). In un ID DIGITALE sono inclusi una chiave privata, memorizzata nel computer del mittente e un certificato (con una chiave pubblica). Il certificato viene inviato quando il mittente inserisce una firma digitale nei messaggi, per consentire l'autenticazione da parte del destinatario.*

Chiave privata: *Chiave segreta memorizzata nel computer del mittente ed utilizzata da quest'ultimo per:*

- *firmare digitalmente i messaggi inviati ai destinatari*
- *decodificare i messaggi provenienti dai destinatari.*

Le chiavi private ***devono essere protette da password.***

E' bene notare che qualora per qualche motivo venisse <u>persa</u> la password, il certificato diventerebbe inutilizzabile.

Chiave pubblica: *Chiave inviata da un mittente ad un destinatario, in modo che il destinatario possa verificare la firma del mittente e assicurarsi che il*

messaggio non sia stato contraffatto. I destinatari utilizzano, inoltre, la chiave pubblica per cifrare i messaggi inviati al mittente.

Un proprietà importante di questo meccanismo è che tra le chiavi esiste una correlazione matematica, tuttavia non è possibile risalire ad una delle due chiavi senza conoscere l'altra.

Azione da compiere	**Chiave usata**	**Di chi?**
Spedire un messaggio firmato	Chiave privata	Di chi spedisce
Autenticare un messaggio firmato ricevuto	Chiave pubblica	Di chi spedisce
Spedire un messaggio criptato	Chiave pubblica	Del ricevente
Decifrare un messaggio criptato	Chiave privata	Del ricevente

Per scaricare una delle guide presenti nel web: crittografia e firma digitale[84]

È possibile ottenere maggiori informazioni sulle caratteristiche di un certificato, ad esempio effettuare le seguenti operazioni:

- *Visualizzare la gerarchia di attendibilità del certificato e controllare l'autorità al vertice della gerarchia che ha rilasciato il certificato.*
- *Determinare l'algoritmo della firma elettronica utilizzato dal certificato, come ad esempio RSA/SHA1.*
- *Determinare l'algoritmo di crittografia utilizzato dal certificato, ad esempio 3DES.*

Per visualizzare le informazioni di un certificato utilizzato per crittografare o apporre una firma digitale a un messaggio di posta elettronica ricevuto, aprire il messaggio e fare clic sul pulsante relativo alla crittografia all'estrema destra

Per scaricare la guida: certificati digitali [85]

E' piuttosto complesso descrivere questa procedura il sistema più semplice che consiglio è provare in pratica tutto il meccanismo scaricando un certificato s-mime.

La GlobalTrust è una delle poche CA, se non ormai l'unica, (***Thawte*** ha cessato di erogare S-/MIME gratuiti dal 2009) che rilasciano certificati S/MIME gratuiti in Italia. Per prendere confidenza

[84] http://www.globaltrust.it/html_popup/pdfguide/ALGORITMICRITTOGRAFICIEFIRMADIGITALE.pdf
[85] https://www.globaltrust.it/html_popup/pdfguide/SpecifichetecnicheCertificatiSSL.pdf

con questa tecnologia è utile scaricare un certificato, che potrà essere fatto dal sito https://www.globaltrust.it/modulo_reg_smime.asp e la procedura, guiderà l'utente gradatamente all'acquisizione del certificato.
Si potrà da subito inviare messaggi e relativi allegati firmati e, volendo, crittografati. La GlobalTrust è l'unica che, una volta acquisito il certificato, fa effettuare una serie di test ***"Keytest"*** seguiti da personale specializzato, il che, per un prodotto gratuito, non è poco. Tutto questo, rappresenta una corretta visione nello spingere la cultura della sicurezza nel WEB, si possono provare i certificati senza limitazione, essi sono infatti identici a quelli acquistati ed hanno una chiave avanzata 2048/256 bit.
Alcune caratteristiche dei certificati S/MIME rilasciati dalla GlobalTrust:

- Sono riconosciuti dal 99% dei programmi client di posta elettronica;
- Permettono di cifrare e firmare digitalmente i messaggi di posta elettronica creati con i software client Microsoft® Outlook Express, Microsoft® Outlook®, Netscape Messenger, Thunderbird ecc. e qualsiasi altro software compatibile con i certificati digitali di tipo S/MIME;
- Legano l'indirizzo di posta elettronica ad una chiave crittografica utilizzata per firmare e cifrare i messaggi di posta elettronica;
- Utilizzano chiavi asimmetriche di ultima generazione 2048/256 bit.

PROCEDURA DI INSTALLAZIONE DEL CERTIFICATO PERSONALE S/MIME RILASCIATO DALLA GLOBALTRUST

Per ottenere il certificato S/MIME personale, rilasciato dalla Globaltrust, è necessario compilare il form online[86] di richiesta del certificato, rigorosamente protetto con certificato SSL per la sicurezza dei vostri dati, con un sistema di autocertificazione consentito in Italia.

86 https://www.globaltrust.it/modulo_reg_smime.asp

Una volta effettuata la richiesta, prima di poter utilizzare il proprio certificato S/MIME per firmare e criptare il contenuto dei messaggi di posta elettronica inviati, è necessario procedere all'installazione del certificato sul proprio PC e configurare opportunamente il proprio client di posta elettronica.

La procedura è similare in tutti i software di posta elettronica e per brevità, è illustrato in dettaglio MS Outlook.

Per installare il certificato seguire i seguenti step:

1. Aprire il proprio client di posta elettronica (es. Outlook 2003);
2. Cliccare su **Posta in arrivo** ed aprire l'e-mail inviata dalla GlobalTrust con oggetto: ***"Ordine per Personal Secure E-mail";***

I: Ordine per Personal Secure Email n.511 - Messaggio (HTML)

Da: GlobalTrust Certificate Services [mailto:certserv@globaltrust.it]
Inviato: giovedì 16/03/2006 16.56
A: mario.rossi@libero.it
Cc:
Oggetto: Ordine per Personal Secure Email n.511

Gentile Mario Rossi,

La ringraziamo per aver scelto il nostro prodotto **GlobalTrust Personal Secure Email** (certificato personale S/MIME per posta elettronica) valido per **12 mesi** .

Abbiamo assegnato alla pratica online il numero d'ordine 511.

La invitiamo a conservare in un luogo sicuro il suo ordine e la password inserita durante la procedura di registrazione online.

Il nostro sistema è collegato con tutti i database governativi del paese, in cui è possibile reperire le informazioni necessarie alla validazione con i nostri servizi "*Five Star Verification Service*" .

Qualora fosse necessaria altra documentazione provvederemo a contattarla.

Una volta completata la procedura, la sua richiesta sarà elaborata entro 2-3 giorni lavorativi. Non appena processato l'ordine riceverà una email contenente tutte le informazioni per l'installazione del suo **Personal Secure Email** di **GlobalTrust**.

Per ulteriori informazioni, non esiti a chiamare il numero +39-0744-441214

Grazie per aver scelto **GlobalTrust**

Cordiali saluti

3. Cliccare su **Posta in arrivo** ed aprire l'e-mail inviata dalla GlobalTrust con oggetto: ***"Il suo certificato Globaltrust Personal Secure E-mail è pronto per l'installazione!"***

Da: GlobalTrust Certificate Services [mailto:certserv@globaltrust.it]   Inviato: giovedì 16/03/2006 16.56
A: mario.rossi@libero.it
Cc:
Oggetto: Il suo certificato GlobalTrust Personal Secure Email è pronto per l' installazione

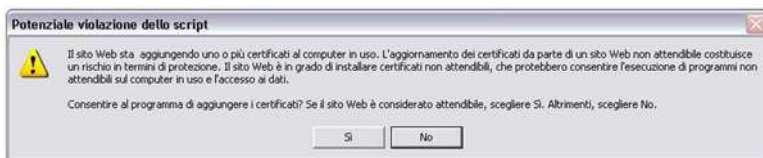
Gentile Mario Rossi,

il suo certificato, che rende possibile la criptazione e la firma digitale delle sue email è pronto ! Il suo S/Mime **GlobalTrust** si integrerà con il Client e-mail esistente.
Cliccando il link sottostante procederà all'installazione dell'applicazione che Le permetterà di installare il certificato in maniera automatica.

Per installare un **Personal Secure Email** di **Globaltrust** utilizzi il seguente link:
https://www.globaltrust.it/check_ccc_sm/coll_inst_cccsm.aspx Non appena richiesto inserisca il numero d'ordine, la password inserita in fase di registrazione e nel campo corrispondente il codice di installazione: **Xb0SIDFuvztV6mqw**.
alla validazione con i nostri servizi "*Five Star Verification Service*".

4. Cliccare sul link (**https...**) per procedere con la fase di installazione del certificato personale S/MIME;

5. Inserire il numero ordine riportato nella e-mail "***Ordine per personal Secure E-mail***" della GlobalTrust e la password inserita nella fase di richiesta del certificato S/MIME personale, fatta precedentemente nel form online;
6. Cliccare sul pulsante **Conferma** per proseguire;
7. Inserire il codice di installazione riportato nella e-mail con oggetto ***"Il suo certificato Globaltrust Personal Secure E-mail è pronto per l'installazione!"***

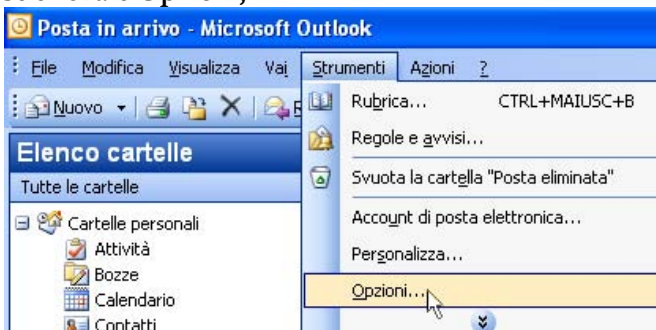
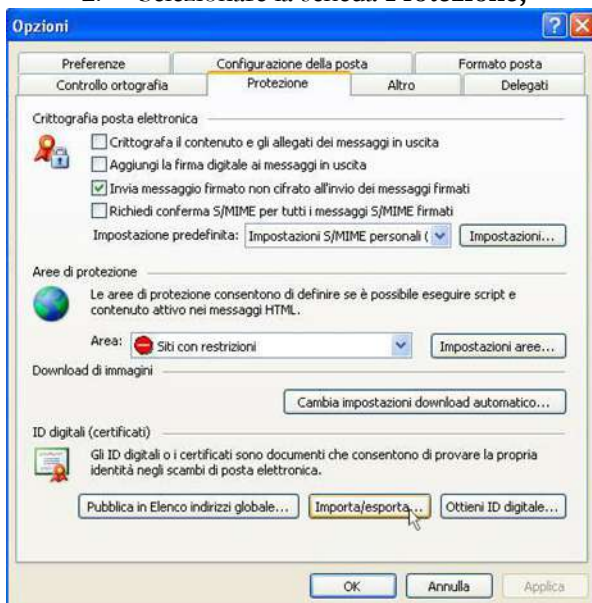
8. Cliccare su **Continua;**
9. E' possibile che venga visualizzato il seguente alert "**Potenziale violazione dello script**";

10. Cliccare su **Si** per continuare;
11. Viene visualizzato a video il seguente messaggio:

12. Cliccare su **OK** per terminare la procedura guidata di installazione. Il certificato personale S/MIME è stato installato correttamente sul PC.

USO DI S/MIME CON SISTEMI CLIENT DI MICROSOFT E THUNDERBIRD

S/Mime in Outlook 2003

Selezionare la voce **Strumenti** dal menù principale;

1. Selezionare **Opzioni;**

2. Selezionare la scheda **Protezione;**

La scheda **Protezione** della finestra di dialogo **Opzioni** viene utilizzata per configurare le opzioni di firma digitale e la crittografia.

Analizziamo in dettaglio le funzioni configurabili :

- **Crittografa il contenuto e gli allegati dei messaggi in uscita:** Selezionare questa casella di controllo se la maggior parte dei messaggi inviati deve essere crittografata e si desidera crittografare tutti i messaggi di posta in uscita, per impostazione predefinita. É possibile ignorare la crittografia di un messaggio specifico cambiando le proprietà del messaggio al momento della sua composizione. Deselezionare questa casella di controllo se la maggioranza dei messaggi in uscita non deve essere crittografata.
  IMPORTANTE: se prima non si è scambiata la chiave pubblica non sarà possibile leggere i messaggi crittografati.

- **Aggiungi la firma digitale ai messaggi in uscita:** Selezionare questa casella di controllo se la maggior parte dei messaggi deve essere firmata e si desidera apporre la firma digitale a tutti i messaggi in uscita per impostazione predefinita. Deselezionare tale casella se più messaggi non devono essere firmati; l'utente potrà poi firmare in modo digitale determinati messaggi al momento della loro composizione.

- **Invia messaggio firmato non cifrato all'invio dei messaggi firmati:** Selezionare questa casella di controllo, se l'utente deve inviare messaggi con firma digitale a destinatari che non hanno la funzione S/MIME, per inviare messaggi con firma digitale e testo non cifrato per impostazione predefinita. È possibile ignorare questa opzione per singoli messaggi al momento della loro composizione. Questa casella può essere per lo più deselezionata, in quanto la maggior parte dei client di posta elettronica supporta lo standard S/MIME.

- **Richiedi conferma S/MIME per tutti i messaggi S/MIME firmati:** Selezionare questa casella di controllo per richiedere una conferma di protezione per tutti i messaggi S/MIME per impostazione predefinita. È possibile ignorare

l'impostazione per singoli messaggi al momento della loro composizione. Una conferma di protezione indica che il messaggio è stato ricevuto e la firma verificata. Nessuna conferma viene inviata se la firma non è stata verificata.

- **Impostazioni:** Fare clic sul pulsante Impostazioni per configurare impostazioni di protezione avanzate e creare gruppi di impostazioni di protezione supplementari. Per ulteriori dettagli vedere il seguente paragrafo "Creare e usare i profili di protezione".

- **Pubblica in Elenco indirizzi globale:** Fare clic su questo pulsante per pubblicare i propri certificati nell'Elenco indirizzi globale, rendendoli disponibili ad altri utenti di **Exchange Server all'interno dell'azienda** che devono inviare messaggi crittografati. Questa opzione rappresenta un'alternativa all'invio ad altri utenti di una copia del proprio certificato.

3. Fare clic su **Impostazioni** per visualizzare la finestra di dialogo **Cambia impostazioni di protezione**.

4. Nella sezione **Certificati e algoritmi>Certificato firma:** cliccare sul pulsante **Scegli...**
5. Dalla finestra di dialogo visualizzata, contenente la lista dei certificati presenti sul PC, selezionare il certificato personale S/MIME (in questo es...)
6. Cliccare su **OK** per confermare.
7. Se il programma non ha inserito automaticamente lo stesso certificato nel campo **Certificato crittografia,** ripetere i passi 5, 6, e 7 per utilizzare il certificato S/MIME per cifrare i messaggi di posta.

Come firmare digitalmente un messaggio di posta elettronica
Firmare digitalmente un messaggio di posta elettronica garantisce autenticazione e integrità dei dati inviati in Rete, in particolare che i dati sono stati scritti dal legittimo mittente e che questi non hanno subito alterazioni/ manomissioni prima di raggiungere il destinatario.
Scrivere un nuovo messaggio ed inserire eventuali allegati

1. Cliccare sul pulsante **Firma**

2. Cliccare sul pulsante **Invia**

ATTENZIONE: Il destinatario deve possedere la chiave pubblica del mittente per poter verificare l'autenticità della firma.

Il modo più semplice per fornirgli la chiave pubblica è allegare automaticamente il certificato ad ogni messaggio di posta firmato.

Questa opzione può essere attivata attraverso i seguenti step:

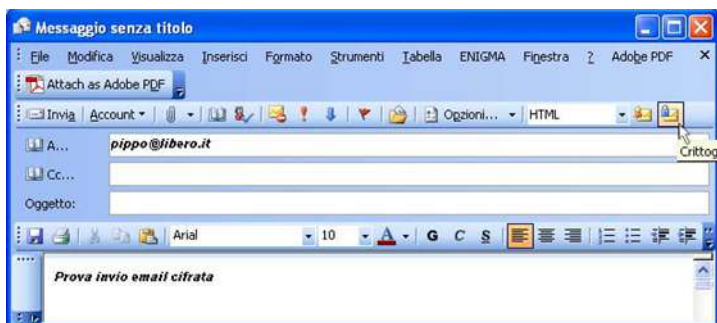
1. Selezionare la voce **Strumenti** dal menù principale
2. Selezionare **Opzioni**

3. Selezionare la scheda **Protezione;**

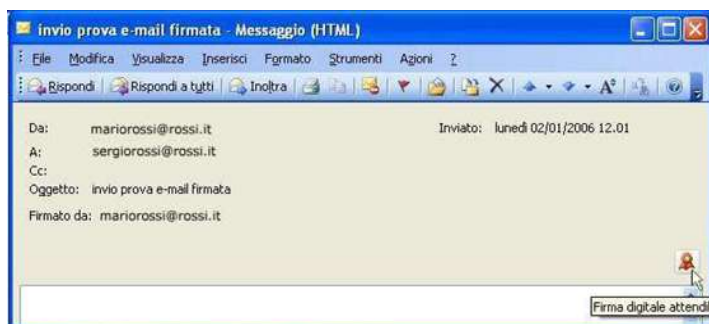
4. Cliccare su **Impostazioni;**
5. Attivare la voce **Invia certificati con messaggi firmati.**

Come cifrare il contenuto di un messaggio di posta elettronica
Cifrare il contenuto di un messaggio di posta elettronica, ed eventuali allegati, garantisce confidenzialità e riservatezza delle informazioni inviate in Rete, in particolare garantisce, che solo il legittimo destinatario possa leggere il contenuto dell'e-mail.

ATTENZIONE: per cifrare un messaggio di posta elettronica è necessario avere la chiave pubblica del destinatario.

1. Scrivere un nuovo messaggio di posta ed inserire eventuali allegati;
2. Verificare se si possiede il certificato digitale del destinatario, andando nella rubrica di OE;
3. Cliccare sul pulsante **Codifica** ;

4. Cliccare sul pulsante **Invia.**

Verifica di una firma digitale

1. Cliccare su **posta in arrivo** ed aprire il messaggio firmato;

2. Verificare la validità della firma nella riga di stato **Firmato da:** Se al di sotto della firma viene visualizzata una riga rossa, la firma non è valida;
3. Per visualizzare ulteriori informazioni sullo stato della firma, fare clic sul pulsante . Se il pulsante viene soltanto selezionato, appare un messaggio simile a quello riportato nella figura sopra:
   - Firma digitale attendibile. Fare clic qui per visualizzare i dettagli

   oppure

- Firma digitale non valida. Fare clic qui per visualizzare i dettagli.

Note:

Una firma digitale potrebbe non essere valida o attendibile per vari motivi.

È ad esempio possibile che il certificato del mittente sia scaduto o sia stato revocato dalla CA (Autorità di Certificazione); oppure che il server di verifica del certificato non sia disponibile. In questi casi è necessario contattare il mittente del messaggio per segnalare il problema.

Come inviare la propria chiave pubblica a terzi

Per poter scambiare, con altri utenti, messaggi di posta elettronica cifrati, si devono avere a disposizione le "chiavi pubbliche" di ciascun utente (certificato digitale dell'utente). Vediamo due esempi che illustrano come inviare ed ottenere la chiave pubblica.

Come inviare la propria chiave pubblica ad un destinatario

Scrivere un nuovo messaggio ed inserire eventuali allegati

1. Cliccare sul pulsante **Firma** ;

2. Cliccare sul pulsante **Invia.**

<u>**ATTENZIONE:**</u> Il destinatario deve possedere la chiave pubblica del mittente per poter verificare l'autenticità della firma.

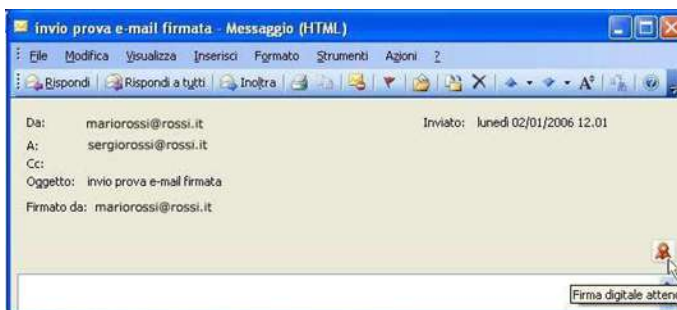
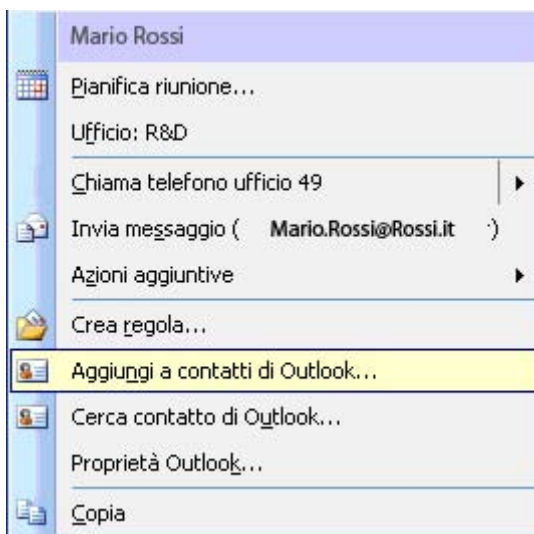
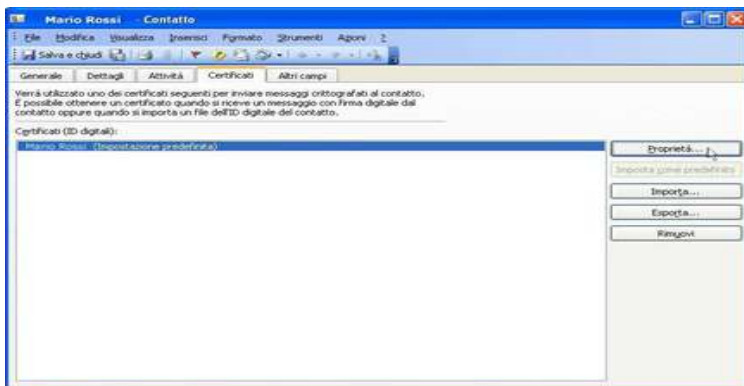
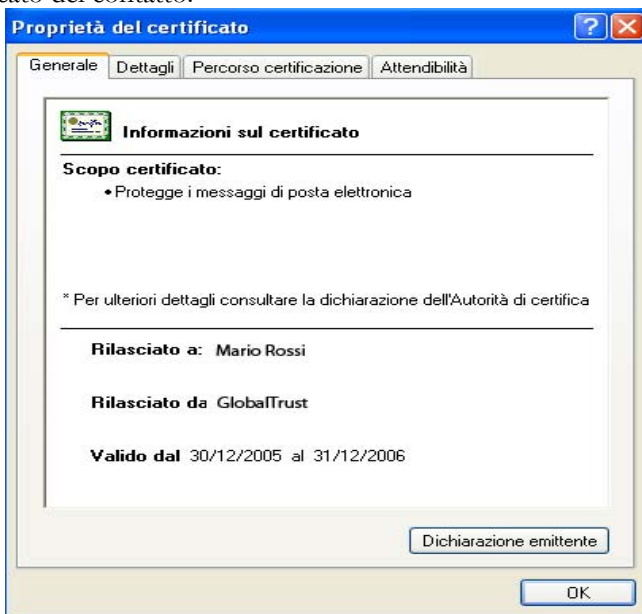
Il modo più semplice per fornirgli la chiave pubblica è allegare automaticamente il certificato ad ogni messaggio di posta firmato. Questa opzione può essere attivata attraverso i seguenti step:

1. Selezionare la voce **Strumenti** dal menù principale;
2. Selezionare **Opzioni;**

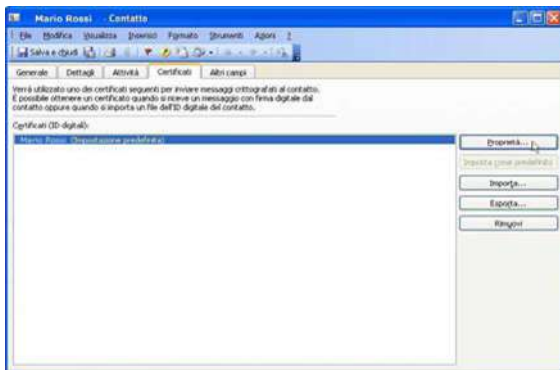
3. Selezionare la scheda **Protezione;**

4. Cliccare su **Impostazioni;**
5. Attivare la voce **Invia certificati con messaggi firmati.**

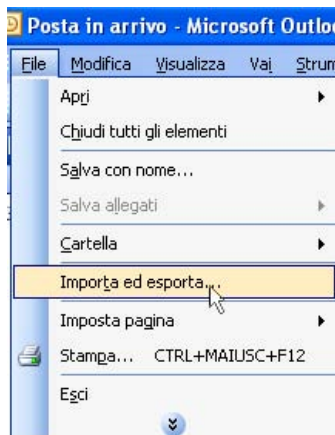
Come ottenere la chiave pubblica di un destinatario:

1. Cliccare su **Posta in Arrivo;**
2. Aprire un messaggio firmato proveniente dal destinatario (Il fatto che il messaggio sia firmato è constatabile dal pulsante presente nel messaggio di posta);

3. Per inserire le informazioni relative al contatto, fare clic con il pulsante destro del mouse sul campo **Da:** e scegliere la voce **Aggiungi a contatti di Outlook;**

4. La chiave pubblica del contatto viene automaticamente associata al contatto stesso, ed è visibile selezionando la scheda **Certificati;**

5. Cliccando su **Proprietà** viene visualizzato in dettaglio il certificato del contatto.

Note:

- Il certificato può essere visualizzato anche cliccando su presente nel messaggio ricevuto.

- Se nel messaggio ricevuto, il certificato del contatto è presente come allegato, mediante un file con estensione **.cer (file contenente un certificato con una chiave pubblica ma nessuna chiave privata),** è possibile, importare manualmente il certificato associato al contatto, cliccando su **Importa. (**viene richiesto di inserire il file con estensione **.cer**, nel quale è memorizzato il certificato del contatto).

Esportare ed importare la lista dei contatti

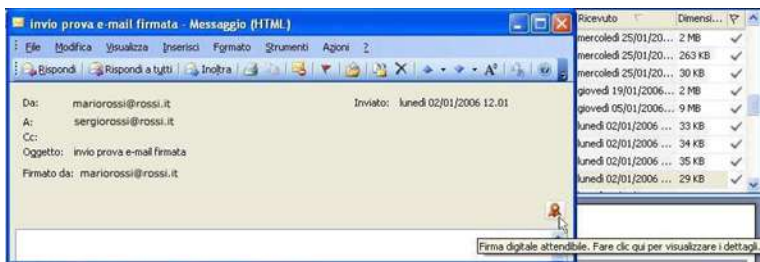
La lista dei contatti può essere esportata e salvata in un file:

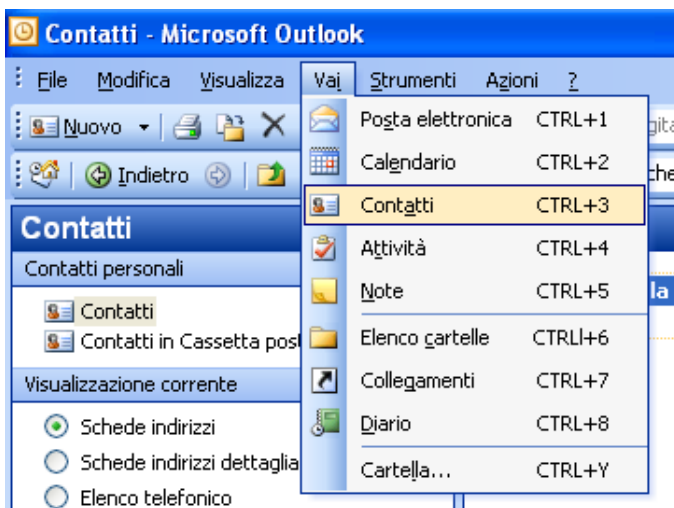
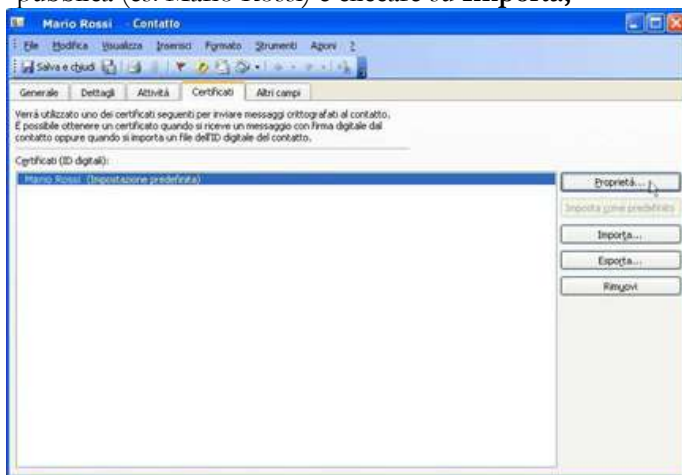
1. Selezionare la voce **File** dalla barra degli strumenti di Outlook;
2. Selezionare la funzione **Importa ed Esporta** dal menù a tendina;

3. Viene lanciato il Wizard che permette di esportare la lista contatti su un file.

ATTENZIONE:

La lista esportata contiene le informazioni di ciascun contatto (ad eccezione delle chiavi pubbliche).

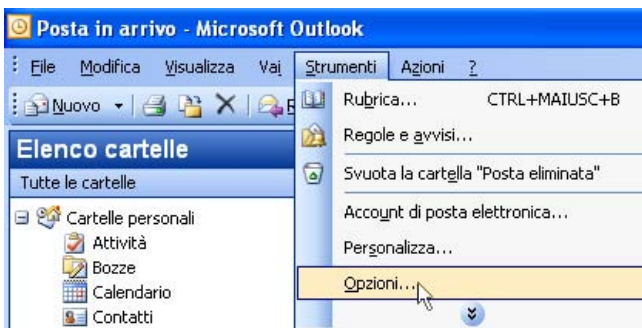
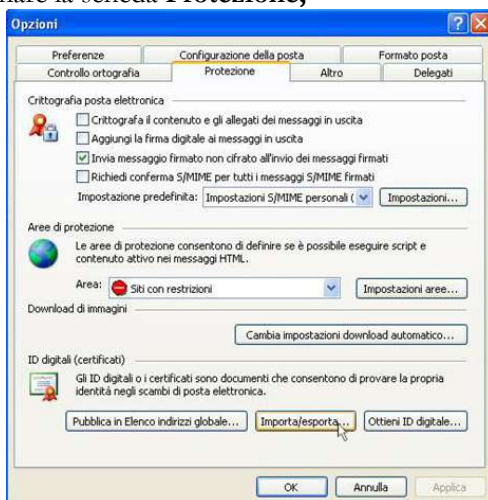
Quindi:
quando viene importata nuovamente la lista dei contatti all'interno della rubrica di Outlook (sfruttando il Wizard **Importa ed Esporta** descritto sopra), è necessario associare a ciascun contatto la relativa chiave pubblica. Due sono i modi possibili:

1. Aprire un messaggio firmato proveniente da un contatto (il fatto che il messaggio sia firmato è constatabile dal pulsante presente nel messaggio di posta. In questo caso è direttamente Outlook ad associare automaticamente il certificato al contatto);

2. Se il certificato del contatto è stato salvato su un file con estensione .cer **(file contenente un certificato con una chiave pubblica ma nessuna chiave privata),** è possibile importare manualmente il certificato associato al contatto:

- Cliccare sulla voce **Vai>Contatti** presente nella barra degli strumenti di Outlook;

- Selezionare il contatto a cui deve essere associata la chiave pubblica (es. Mario Rossi) e cliccare su **Importa;**

- Selezionare il file con estensione **.cer** contenente la chiave pubblica del contatto.

Come esportare il proprio certificato personale S/MIME da Outlook 2003

Questa procedura viene utilizzata quando si vuole fare una copia di backup del proprio certificato personale S/MIME, **procedura altamente raccomandata, a condizione che si protegga il certificato con password.**

1. Selezionare la voce **Strumenti** dal menù principale;
2. Selezionare **Opzioni;**

3. Selezionare la scheda **Protezione;**

4. Cliccare su **Importa/Esporta;**

5. Nella finestra visualizzata, attivare la voce **Esporta ID digitale in un file;**

6. Cliccare su **Seleziona** e scegliere il certificato personale da esportare (inclusa la chiave privata);
7. Cliccare su **Sfoglia** ed inserire la directory di output e nome del file in cui sarà salvato il certificato (il file ha come estensione **.pfx = File contenente un certificato con una chiave pubblica e chiave privata);**
8. Inserire la password associata al certificato (la password in questione è stata utilizzata per proteggere la chiave privata);

ATTENZIONE: **<u>Se per qualche motivo viene persa la password, il certificato diventa inutilizzabile</u>**

9. se si desidera eliminare dal sistema il certificato esportato, attivare la voce **elimina ID digitale dal sistema;**
10. Cliccare **OK** per terminare la procedura.

Come importare il proprio certificato personale S/MIME in Outlook 2003

1. Selezionare la voce **Strumenti** dal menù principale;

2. Selezionare **Opzioni;**

3. Selezionare la scheda **Protezione;**

4. Cliccare su **Importa/Esporta;**

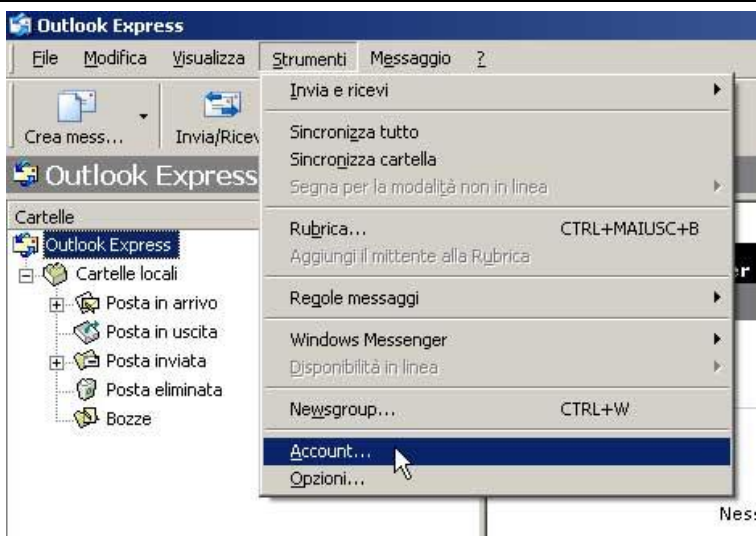
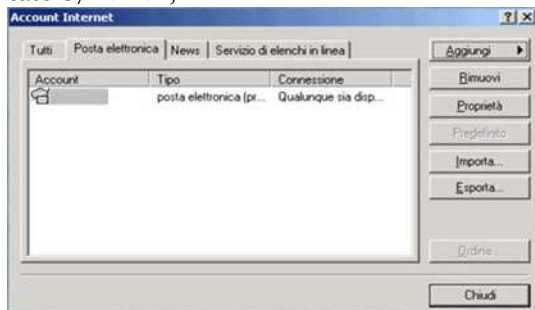
5. Cliccare su **Sfoglia** e selezionare il file con estensione **.pfx** contenente il certificato personale da importare;
6. Digitare la password associata alla chiave privata del certificato;
7. Inserire il nome con cui si desidera salvare il certificato dentro Outlook;
8. Cliccare su **OK** per terminare la procedura.

Installazione e utilizzo della posta elettronica certificata con Outlook Express 5

Come associare il certificato S/MIME personale ad un account di posta elettronica:

1. Aprire Outlook Express;

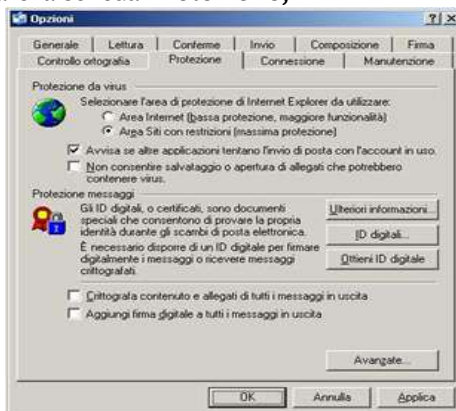
2. Selezionare la voce **Strumenti** dalla barra degli strumenti;

3. Selezionare la voce **Account...**dal menù a tendina;

4. Nella finestra di dialogo visualizzata, selezionare la voce **Posta Elettronica** e selezionare l'account a cui si vuole associare il certificato S/MIME;

5. Cliccare su **Proprietà;**
6. Cliccare sulla scheda **Protezione**;
7. Cliccare su **Seleziona certificato di firma** e dalla finestra di dialogo che viene aperta, contenente la lista dei certificati installati sul PC, selezionare il certificato personale S/MIME;
8. Cliccare su **Seleziona certificato per la codifica** e dalla finestra di dialogo che viene aperta, contenente la lista dei certificati installati sul PC, selezionare di nuovo il certificato personale S/MIME;

9. Cliccare su **OK** per terminare la procedura e tornare ad Outlook Express.

<u>ATTENZIONE</u>: Il destinatario deve possedere la chiave pubblica del mittente per poter verificare l'autenticità della firma.
Il modo più semplice per fornirgli la chiave pubblica è allegare automaticamente il certificato ad ogni messaggio di posta firmato.

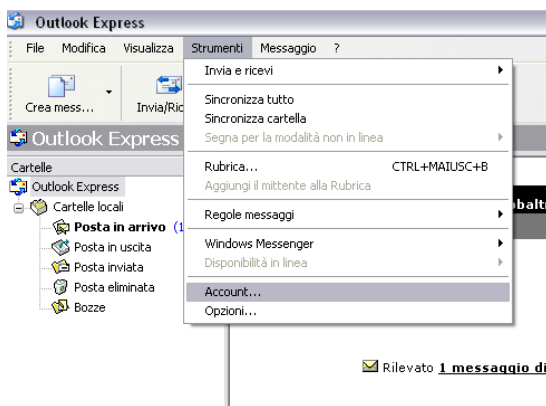
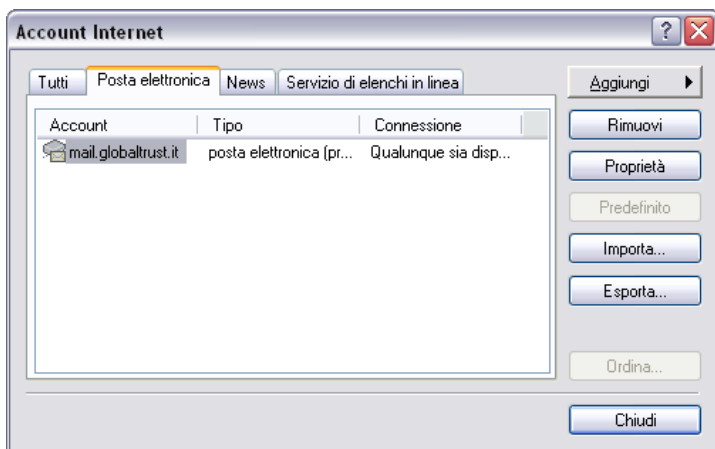
1. Selezionare la voce **Opzioni** dal menù **Strumenti;**

2. Selezionare la scheda **Protezione;**

3. Cliccare sul pulsante **Avanzate**;

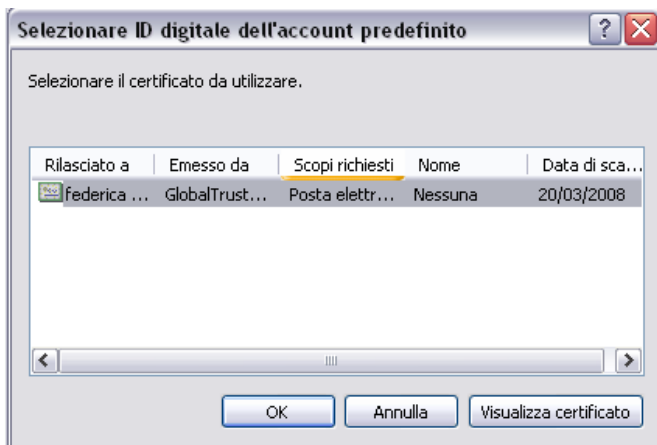
4. Attivare la voce ***Invia certificati con messaggi firmati.***

Installazione e utilizzo della posta elettronica certificata con Outlook Express 6

Come associare il certificato S/MIME personale ad un account di posta elettronica:

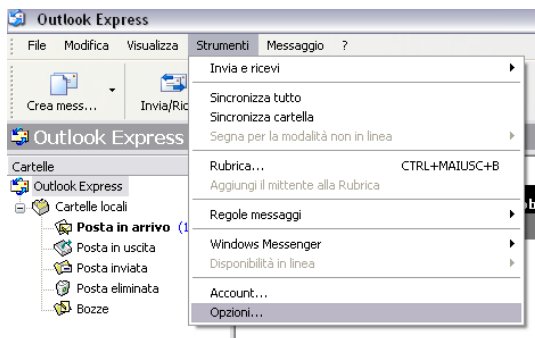
1. Aprire Outlook Express 6;
2. Selezionare la voce **Strumenti** dalla barra degli strumenti;
3. Selezionare la voce **Account...**dal menù a tendina;

4. Nella finestra di dialogo visualizzata, selezionare la voce **Posta Elettronica** e selezionare l'account a cui si vuole associare il certificato S/MIME;

5. Cliccare su **Proprietà;**

6. Nella finestra Proprietà, cliccare sulla scheda **Protezione;**

7. Premere il tasto **Seleziona** per selezionare il Certificato per la Firma Digitale;

8. Nella finestra visualizzata scegliere il certificato da utilizzare;

9. Premere **OK**;
10. Ripetere i passi 7-8-9 per selezionare il Certificato per la Crittografia;
11. Premere **OK**, per completare la procedura e tornare ad Outlook Express.

ATTENZIONE: Il destinatario deve possedere la chiave pubblica del mittente per poter verificare l'autenticità della firma.
Il modo più semplice per fornirgli la chiave pubblica è allegare automaticamente il certificato ad ogni messaggio di posta firmato.

1. Selezionare la voce **Opzioni** dal menù **Strumenti;**

2. Selezionare la scheda **Protezione;**

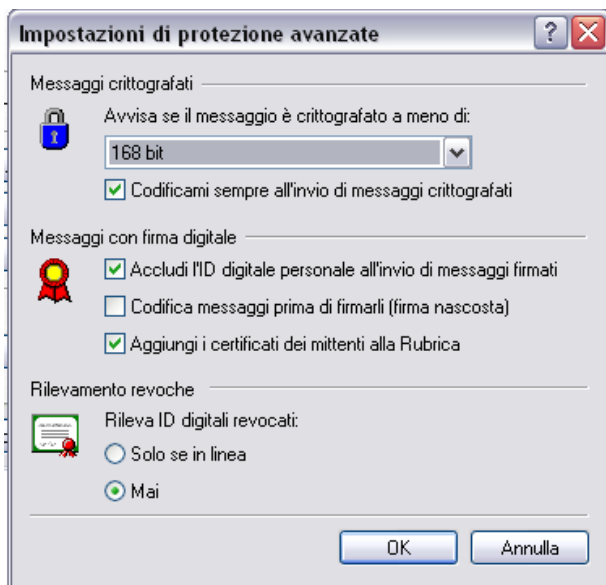
3. Attivare la voce **Aggiungi firma digitale a tutti i messaggi in uscita;**
4. Premere **OK**.

Come aggiungere il certificato di un destinatario all'elenco dei contatti

Per aggiungere automaticamente un certificato digitale associato ad un contatto presente nella rubrica di OE:

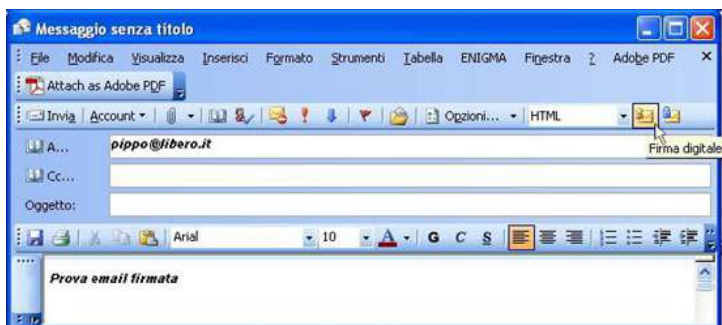
1. Selezionare la voce **Opzioni** dal menù **Strumenti;**

2. Selezionare **Protezione;**

3. Cliccare sul pulsante **Avanzate;**

4. Attivare la voce *Aggiungi il Certificato dei mittenti alla Rubrica*. In questo modo, quando si ricevono messaggi di posta elettronica certificati, il certificato associato al mittente viene automaticamente registrato all'interno della rubrica.

Come firmare digitalmente un messaggio di posta elettronica:
Firmare digitalmente un messaggio di posta elettronica garantisce autenticazione e integrità dei dati inviati in Rete, in particolare garantisce che i dati siano stati scritti dal legittimo mittente e che questi non abbiano subito alterazioni/ modifiche non autorizzate prima di raggiungere il destinatario.

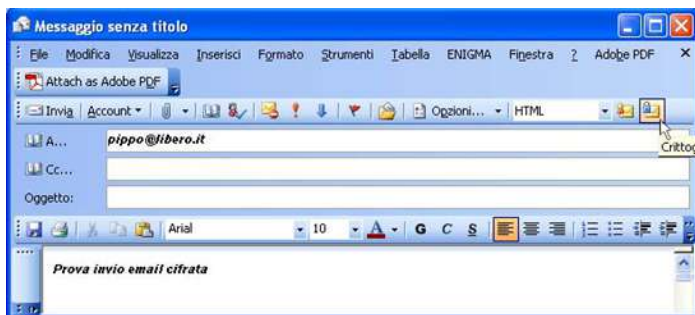
Scrivere un nuovo messaggio di posta ed inserire eventuali allegati:

1. Cliccare sul pulsante **Firma digitale** ;

2. Cliccare sul pulsante **Invia.**

Come cifrare il contenuto di un messaggio di posta elettronica
Cifrare il contenuto di un messaggio di posta elettronica garantisce confidenzialità e riservatezza delle informazioni inviate in Rete, in particolare garantisce che solo il legittimo destinatario possa leggere il contenuto delle e-mail (inclusi eventuali allegati).

1. Scrivere un nuovo messaggio di posta elettronica ed inserire eventuali allegati;

2. Verificare se si possiede il certificato digitale del destinatario, andando nella rubrica di OE;

3. Cliccare sul pulsante **Crittografa messaggio** ;

4. Cliccare sul pulsante **Invia.**

S/MIME CON SISTEMI DI WEB MAIL: GMAIL

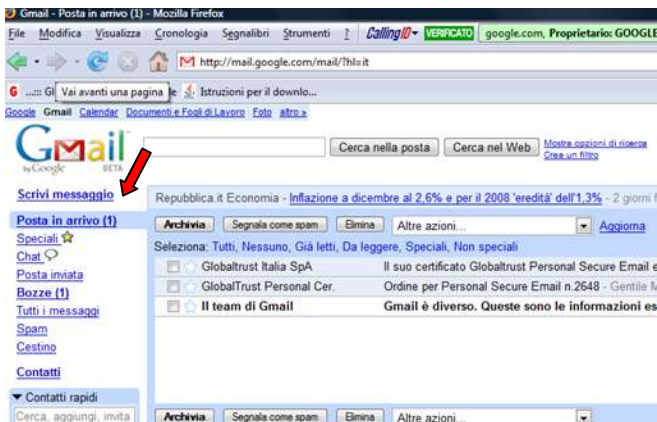
L'esigenza di inviare e-mail sicure è particolarmente sentita da GOOGLE, che è stata pioniera nell'abilitare tutti gli account di posta elettronica alla firma digitale.
Si può, quindi, installare il certificato relativo su un account web seguendo le indicazioni qui appresso:

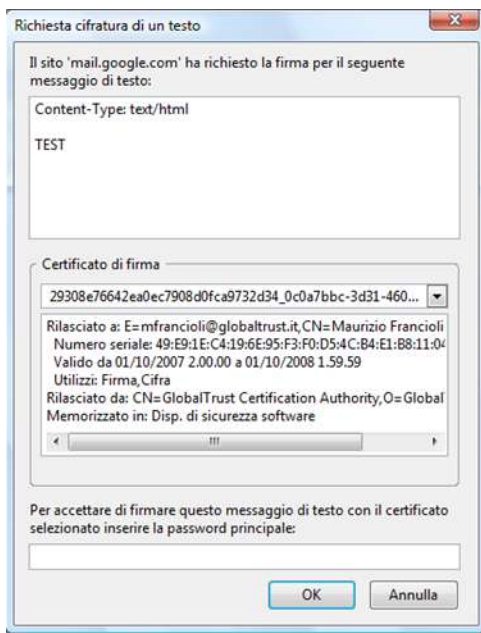
Firma Digitale con Gmail

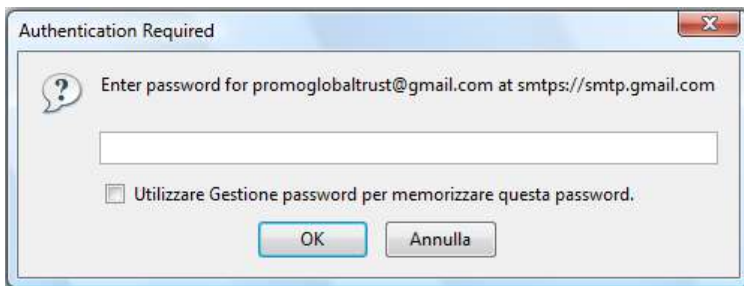
Step 1
Per primo bisogna aggiornare Firefox con un nuovo componente aggiuntivo. Tale componente si può scaricare all'indirizzo:
https://addons.mozilla.org/it/firefox/addon/592;

Step 2
Una volta scaricato il componente aggiuntivo (gmail_s_mime-0.3.0-fx.xpi), per installarlo, basterà avviare Firefox ed eseguire la seguente procedura:

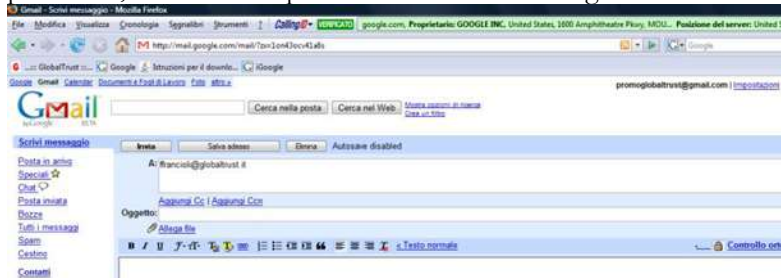
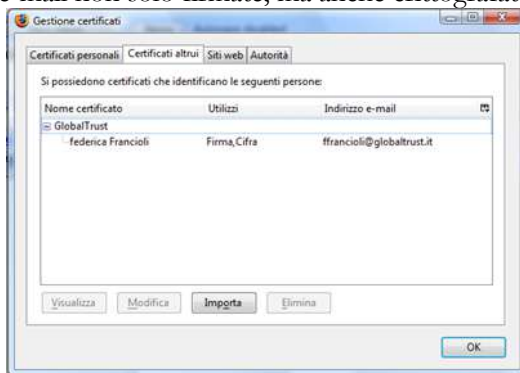
File → Apri File… → selezionare il file - OK → Installa Adesso

Finita la procedura, Firefox sarà compatibile e in grado di supportare il portale di Gmail con la sua nuova funzione di Firma Digitale.
A questo punto accedendo al portale di Gmail attraverso il browser Firefox, si potrà usufruire del servizio di firma digitale. Una volta entrati nel portale di Gmail basterà scrivere una nuova e-mail per vedere la nuova funzione di firma digitale.

Una volta scelto di scrivere una nuova e-mail, ci si troverà di fronte alla tradizionale finestra dell'editor di Gmail, ma nel lato destro della barra delle funzioni si noterà il bottone che permette di firmare digitalmente la e-mail, nonostante sia all'interno di un client web di posta.

Preparata l'e-mail e attivata la funzione di Firma Digitale, cliccando su **Invia,** verrà mostrata la seguente finestra, dove sono riassunti i dati del certificato usato per la firma.

In fondo alla finestra verrà richiesta la password di protezione del certificato, stabilita in fase di esportazione dello stesso.

Premendo poi OK, si accede alla seguente finestra:

Infine nella finestra soprastante verrà chiesto di inserire la password di accesso utilizzata per l'account Gmail. Premuto OK, l'e-mail firmata digitalmente verrà inviata.

E-mail crittografate con Gmail

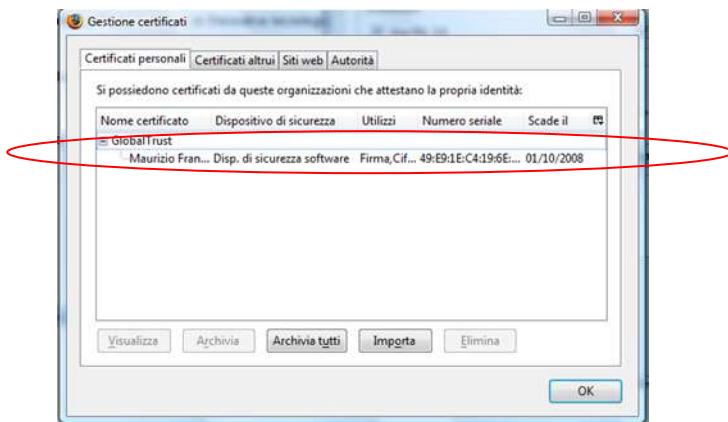
Il client di posta Gmail non consente solo di firmare digitalmente un'e-mail, ma permette anche di crittografarla, rendendola ancora più sicura e riservata. Infatti, in Gmail, come in un comune client di posta tipo Outlook, è possibile lo scambio delle rispettive chiavi pubbliche, consentendo poi di inviarsi e-mail crittografate.

Come si può vedere di seguito, il portale Gmail, al momento in cui riceve un'e-mail firmata digitalmente, salva la chiave pubblica del mittente e nella sezione "certificati altrui" di Firefox si troverà il certificato dello stesso. Questo, associato al fatto di rispondere a nostra volta con un'e-mail firmata digitalmente, ci darà la possibilità di scambiare e-mail non solo firmate, ma anche crittografate.

Nota

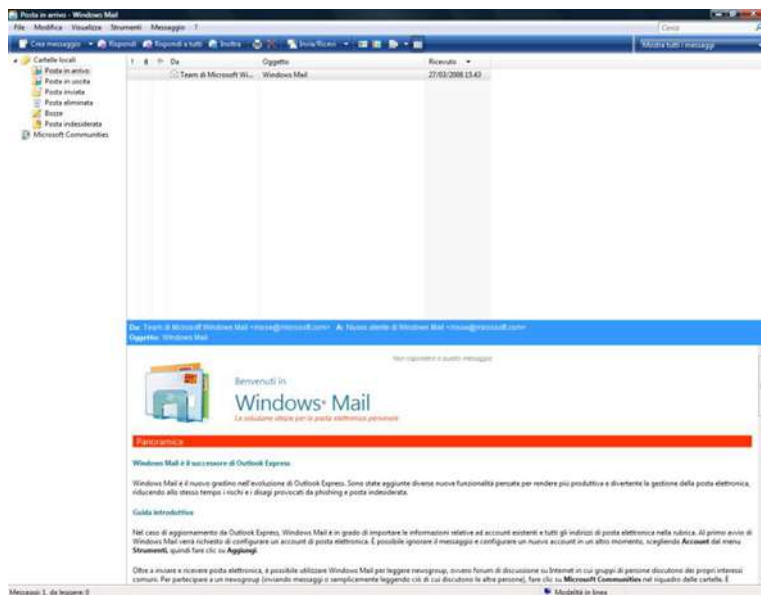
la procedura appena spiegata è realizzabile solo attraverso il browser Firefox, e quindi i certificati digitali installati nel PC, devo essere visibili anche da Firefox e non solo da Internet Explorer. Per far questo, occorre esportare il certificato da IE e importarlo in Firefox.

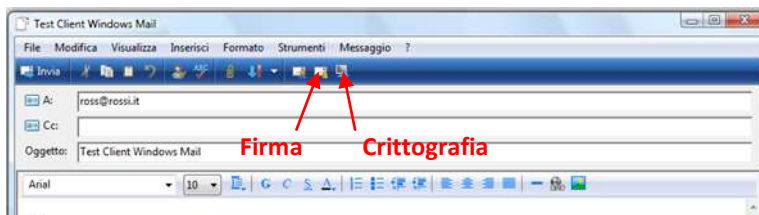
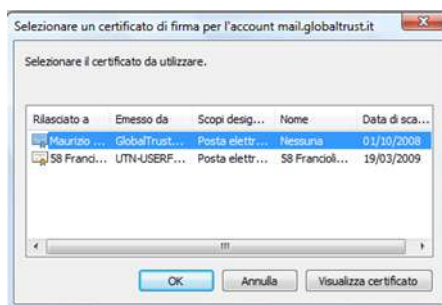
ESPORTAZIONE E IMPORTAZIONE DI UN CERTIFICATO DIGITALE

Di seguito è riportato come esportare un certificato da Internet Explorer ed importarlo in Firefox.

Step 1
<u>**Avvio Internet Explorer**</u>
Strumenti → Opzioni Internet → Contenuto → Certificati → Esporta
Seguendo questa procedura esporteremo il certificato, salvandolo in un file con estensione .pfx. Durante la fase di esportazione ci verrà chiesta una password di protezione del certificato ed è importante non dimenticarla, in quanto ci verrà richiesta sia in fase di importazione, che in fase di invio dell'e-mail firmata digitalmente dal portale Gmail, come indicato nella guida precedente.

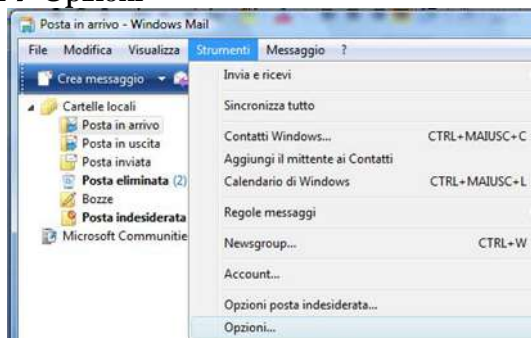
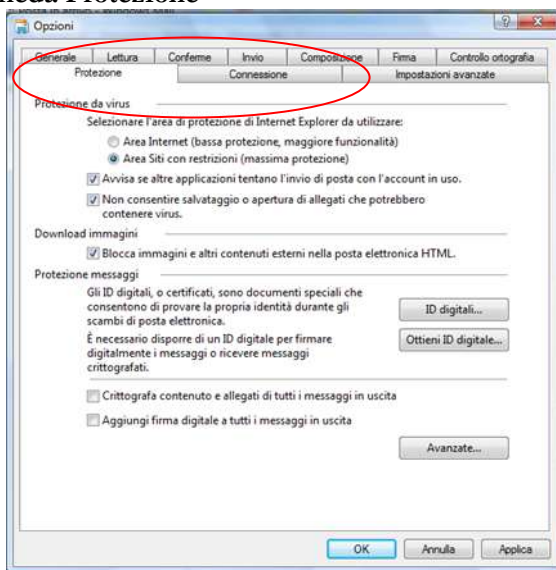
Step 2
<u>**Avvio Firefox**</u>
Strumenti → Opzioni → Avanzate → Cifratura → Mostra Certificati → Importa
Seguita la procedura, basterà specificare il file contenente il certificato, inserire la password di protezione, e il certificato sarà importato e perfettamente visibile anche da Firefox.

S/MIME con Windows Mail

Windows Mail è il nuovo client di posta introdotto con Windows Vista, nonché l'evoluzione di Outlook Express. Di seguito verrà riportato come utilizzare correttamente Windows Mail con i certificati digitali S/MIME.

La caratteristica principale di questo client di posta è che non richiede particolari configurazioni per impiegare i certificati digitali S/MIME e quindi per inviare e-mail firmate digitalmente e/o crittografate.

Windows Mail consente, da "subito", di inviare e-mail firmate e/o crittografate e lo si può notare dal fatto che nel creare una nuova e-mail nella barra degli strumenti, sono subito presenti e attivi i relativi bottoni:

Solo dopo aver stabilito se firmare digitalmente e/o crittografare l'e-mail, verrà chiesto con quale certificato digitale, mostrando la lista dei certificati installati nel PC:

Questo eviterà di stabilire e assegnare precedentemente con quale certificato firmare le e-mail, operazione che era invece necessaria con Outlook Express.

Windows Mail è in grado infatti di "vedere" e impiegare i certificati installati nel PC, purché questi siano installati in Internet Explorer, caratteristica che preclude che i certificati siano richiesti ed installati con Explorer o in caso contrario, vengano poi importati in Internet Explorer.

Nella sezione strumenti di Windows Mail è possibile stabilire delle opzioni riguardanti i certificati digitali:

Strumenti→ Opzioni

Nella scheda Protezione

Possiamo stabilire se inviare tutti i messaggi in uscita firmati e/o crittografati.

S/MIME in Windows Live Mail

Apporre una firma digitale o crittografare i messaggi

Se ad un account di posta elettronica è associato un ID digitale[87], si può utilizzare Windows Live Mail per aggiungere ai messaggi una Firma Digitale[88] con la quale confermare la propria identità, oppure inviare un messaggio di posta elettronica crittografato per impedire ad altri di leggere la propria posta.

Per inviare messaggi di posta elettronica crittografati, occorre associare un ID digitale al proprio nome nella rubrica.
Per impostazione predefinita, Windows Live Mail aggiunge automaticamente gli ID digitali nei contatti nella rubrica, quando ci vengono inviati messaggi con firma digitale.

1. Avvia Windows Live Mail.
   a. In Windows XP fare clic sul pulsante Start, quindi su Programmi.

–oppure–

In Windows Vista fare clic sul pulsante Start, quindi su Tutti i programmi.
   b. Fare clic su Windows Live, quindi su Windows Live Mail;
2. Scegliere Opzioni per la protezione dal menu Strumenti; se la barra dei menu non è visualizzata, nella barra degli strumenti fare clic sul pulsante Mostra menu, quindi su Mostra tutti i menu;
3. Nella scheda Protezione fai clic su Ottieni ID digitale;
4. Verrà aperta una pagina Web contenente le autorità di certificazione. Seleziona un'autorità, quindi segui le istruzioni visualizzate sullo schermo. L'autorità di certificazione ti invierà tramite posta elettronica l'ID digitale e le relative istruzioni.

1. **Avvia Windows Live Mail**
   a. In Windows XP fare clic sul pulsante Start, quindi su Programmi.

–oppure–

[87] http://help.live.com/help.aspx?project=wl_mailv2&market=it-it&querytype=topic&query=outlookexpresslivev1_proc_encryptmessages.htm
[88] http://help.live.com/help.aspx?project=wl_mailv2&market=it-it&querytype=topic&query=outlookexpresslivev1_proc_encryptmessages.htm

In Windows fare clic sul pulsante Start, quindi su Tutti i programmi.

b. Fare clic su Windows Live, quindi su Windows Live Mail;

2. Per creare un nuovo messaggio di posta elettronica scegliere Nuovo nella barra degli strumenti di Windows Live Mail;
3. Nella finestra del messaggio apri il menu Strumenti. Se la barra dei menu non è visualizzata, nella barra degli strumenti fare clic sul pulsante Mostra menu, quindi su Mostra tutti i menu;
4. Per aggiungere una firma digitale al messaggio scegliere Firma digitale.

–oppure–

Per crittografare il messaggio, scegliere Crittografa. Non si può inviare un messaggio crittografato ad un contatto se non si dispone del suo ID digitale nella rubrica.

Aggiungere automaticamente una firma digitale a tutti i messaggi di posta elettronica o crittografarli[89]

1. Avviare Windows Live Mail.
   a. In Windows XP fare clic sul pulsante Start, quindi su Programmi.

–oppure–

In Windows Vista fare clic sul pulsante Start, quindi su Tutti i programmi.

b. Fare clic su Windows Live, quindi su Windows Live Mail;

2. Scegliere Opzioni per la protezione dal menu Strumenti;

Se la barra dei menu non è visualizzata, nella barra degli strumenti fare clic sul pulsante Mostra menu, quindi su Mostra tutti i menu;

3. Nell'area Protezione messaggi della scheda Protezione selezionare le opzioni desiderate;
4. Scegli OK.

Note

- Quando si inviano o si ricevono messaggi crittografati o con Firma Digitale, essi sono contrassegnati con l'icona Firma o Crittografa. Per visualizzare ulteriori dettagli, fare clic sull'i-

[89] http://help.live.com/help.aspx?project=wl_mailv2&market=it-it&querytype=topic&query=outlookexpresslivev1_proc_encryptmessages.htm

cona nel messaggio di posta elettronica. Se si verificano dei problemi con la firma digitale o la crittografia di un messaggio di posta elettronica in arrivo, nella finestra del messaggio viene visualizzato un avviso.

- Se si tenta di inviare un messaggio crittografato o con firma digitale e non si dispone di un ID digitale, Windows Live Mail chiede di crearne uno.
- Si può inoltre ottenere l'ID digitale di terzi scaricandolo dal sito Web di un'autorità di certificazione. (GlobalTrust Personal Digital Certificate and S/MIME[90]).
- Per visualizzare gli ID digitali associati a un contatto presente nella propria rubrica o per importare in essa ID digitali, scegliere Contatti dal menu Strumenti. Nell'elenco dei contatti fare doppio clic su un contatto, quindi clic sulla scheda ID.

Rinnovo delle chiavi e dei certificati

Ciascun certificato digitale e la relativa chiave privata associata, ha un tempo di validità limitato (normalmente un anno). Per il rinnovo del certificato è necessario contattare direttamente la CA (**GlobalTrust**).

FIRMA DEI DOCUMENTI E DEGLI ALLEGATI IN UN MESSAGGIO DI POSTA ELETTRONICA

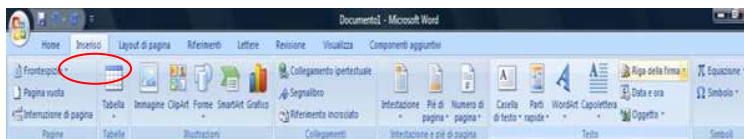
Un aspetto importante, della posta elettronica certificata con S/Mime, è che spesso al messaggio debbono essere allegati documenti di vario genere e di vario formato, Adobe è da sempre il leader nella preparazioni di documenti sicuri e firmati digitalmente.

Microsoft, da non molto, ha seguito questa impostazione, ancora di più nel nuovo Office 2010, dove la firma digitale e la crittografia hanno avuto la dovuta importanza consentendo l'utilizzo della stessa in tutti i programmi di Office.
Si potranno quindi allegare al messaggio, oltre ai documenti in word, anche fogli di calcolo, presentazioni in Power Point ed altro ancora.

[90] https://www.globaltrust.it/modulo_reg_smime.asp

Firma Digitale di un Documento Microsoft Word 2007

Step 1

scheda **Inserisci -** sezione **Testo - Riga della Firma.**

Step 2

Premere **OK**

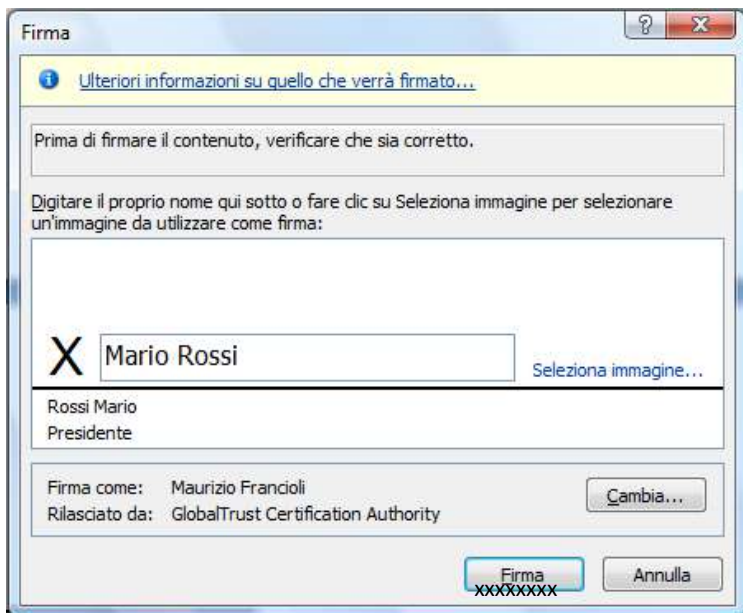
Compilare i campi per l'impostazione della firma:

Step 3

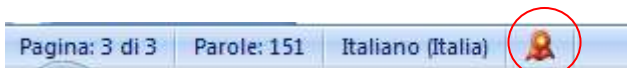
Premuto **OK**, comparirà nel documento la firma con i dati inseriti:

A questo punto cliccando due volte su tale firma, si può digitalizzarla dandole valore legale, con l'ausilio del Certificato Digitale.

Step 4
Dopo aver cliccato due volte sulla firma comparirà la seguente finestra:

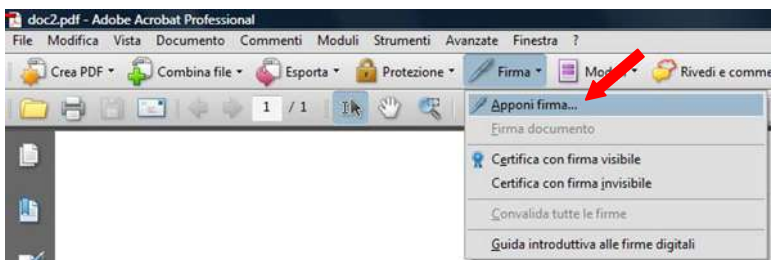
Dopo aver premuto **OK** comparirà la seguente finestra:

Nella casella di testo, a fianco della **X,** andrà digitato il nome del firmatario, in alternativa, si potrà scegliere di inserire un'immagine della firma. Con il tasto **Cambia** si potrà scegliere il certificato da usare per la Firma Digitale. Premendo su **Firma** si va ha ultimare la procedura.

Ultimata la procedura sarà visibile nel documento la Firma Digitale:

Si avrà conferma, della Firma Digitale nel documento, dalla coccarda presente nella barra di stato di Word:

Nota*: affinché il certificato sia visto da Microsoft Word, e quindi impiegato per firmare digitalmente i documenti, deve essere installato in Internet Explorer. Qualora il certificato fosse stato installato con un diverso browser, occorrerà e-sportare il certificato ed importarlo in Internet Explorer.*

Firma Digitale di un Documento PDF

<u>Adobe Acrobat 8</u>

Step 1:
Cliccare sul tasto **Firma** della barra degli strumenti, successivamente cliccare su **Apponi firma**…

Step 2:
Tenendo premuto il tasto sinistro del mouse selezionare l'area dove si vuole apporre la firma.

Step 3:
Selezionata l'area per la firma, comparirà la finestra con le informazioni relative al certificato digitale impiegato per la firma del documento:

Qualora si possedessero più certificati digitali, dal menù a tendina del campo **ID digitale** si potrà selezionare il certificato da impiega-

re. Si conclude la procedura cliccando sul tasto **Firma** e salvando il documento.

Step 4:

Comparirà nell'area prestabilita la Firma Digitale:

Maurizio Franci

Firmato digitalmente da Maurizio Franci
ND: cn=Maurizio Franci
email=[illegible]@globaltrust.it
Data: 2008.05.08 15:01:24 +02'00'

A questo punto il documento sarà firmato digitalmente. Cliccando sulla firma, si aprirà una finestra in cui sono riportate le informazioni relative al certificato digitale.

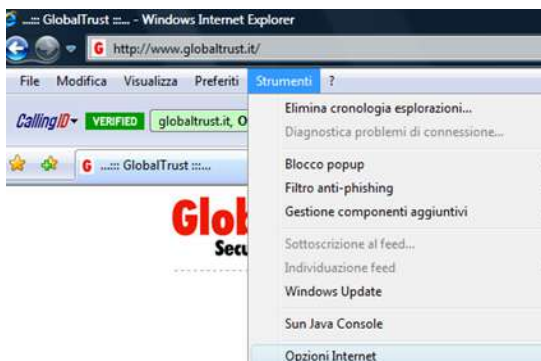
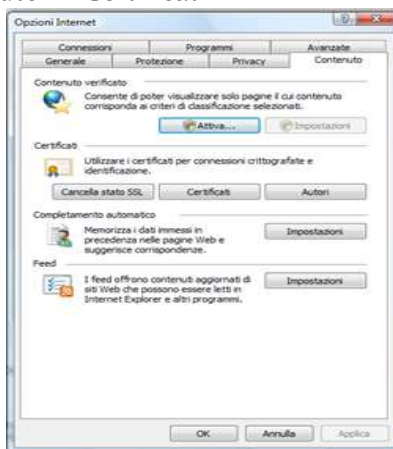
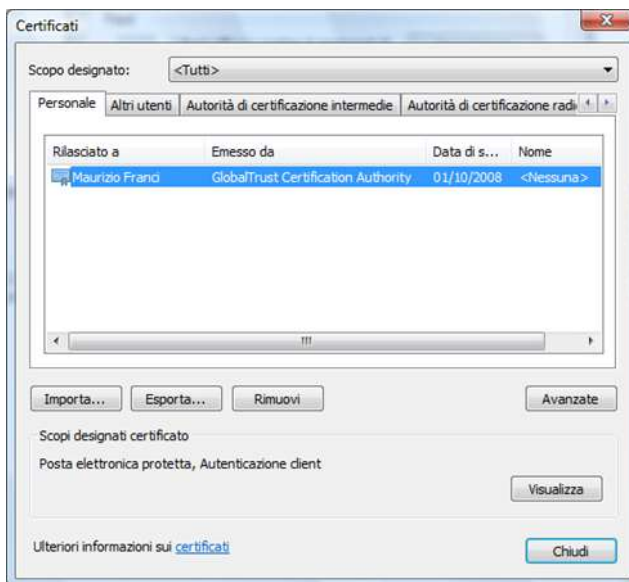
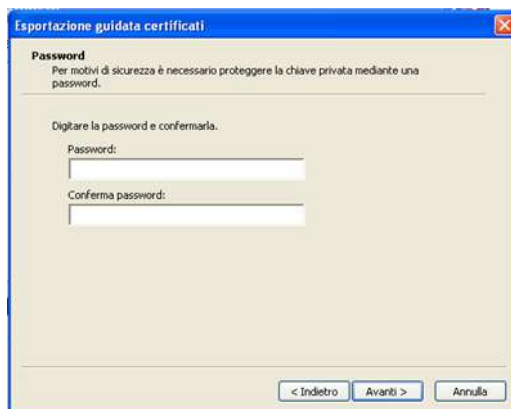
Nota: *affinché il certificato sia visto da Adobe Acrobat, e quindi impiegato per firmare digitalmente i documenti, deve essere installato in Internet Explorer. Qualora il certificato fosse stato installato con un diverso browser, occorrerà esportare il certificato ed importarlo in Internet Explorer.*
Le ultime versioni di Adobe consentono un'infinità di varianti da aggiungere alla firma digitale; si potranno aggiungere infatti, immagini ed altre informazioni, oltre alla possibilità di aggiungere "la marca temporale TIME STAMPING", dando così valenza legale alla data e all'ora della firma del documento.

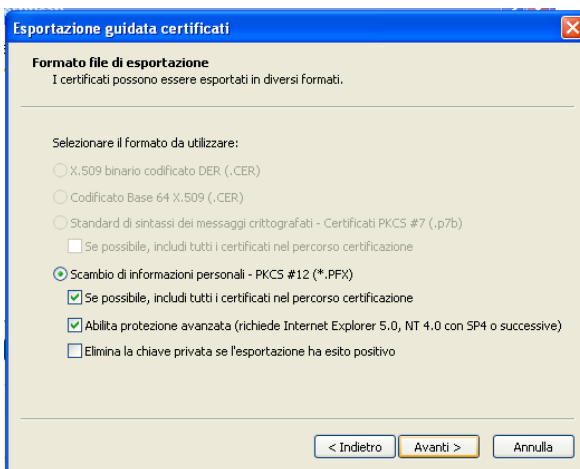
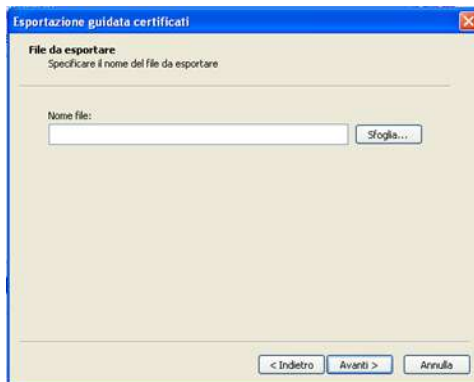
IMPORTAZIONE, ESPORTAZIONE, BACKUP E RIPRISTINO DI UN CERTIFICATO S/MIME

Si è visto come sia importante effettuare una copia di backup del certificato S/MIME e del relativo ripristino dello stesso, essendo importante la portabilità del certificato, come di un documento di identità, e la conservazione sicura dello stesso, ma è bene capire come fare. Il file dove è contenuto il certificato ha un formato particolare ed anche per ragioni di sicurezza, non è consentita la normale copia dello stesso, sono quindi attuate le funzioni di *importazione ed esportazione* per permettere la stessa cosa in modo sicuro. Per ovviare al problema di un eventuale guasto del PC, formattazione o circostanze analoghe che possono causare la perdita del certificato digitale, esso può essere salvato in una copia di backup, che consentirà di ripristinarlo. Il backup del certificato avviene attraverso il browser utilizzato per richiedere ed installare il certificato. Qui di seguito saranno riportate le procedure di backup attraverso i due browser attualmente più diffusi, Internet Explorer e Firefox.

Backup con Internet Explorer 7

Step 1:
Avviare **Internet Explorer**

Step 2:
Nella barra degli strumenti premere: **Strumenti → Opzioni Internet**

Step 3
Scheda: **Contenuto → Certificati**

Step 4
Nella sezione **Personale** si trovano tutti i certificati personali installati, quindi selezionare il certificato da esportare e cliccare su **Esporta**, per avviare l'esportazione:

Step 5
Selezionare l'opzione: **Esporta la chiave privata**

Step 6

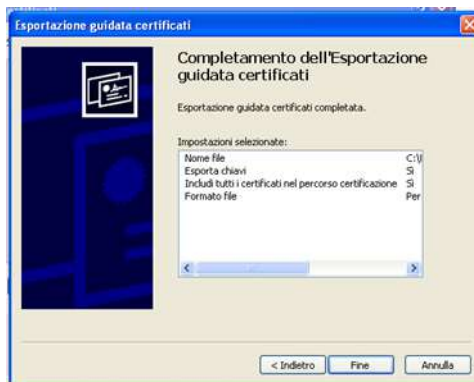
Selezionare l'opzione: **Se possibile, includere tutti i certificati nel percorso certificazione** e **Abilita protezione avanzata**

Step 7

Scegliere la password di protezione della chiave privata del certificato:

***Nota**: è importante non dimenticare la password, in quanto sarà necessaria per ripristinare il certificato.*

Step 8

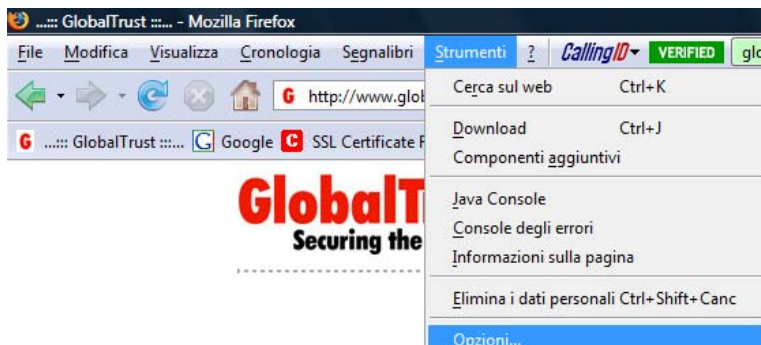
Con il tasto **Sfoglia**, stabilire destinazione e nome del file di backup:

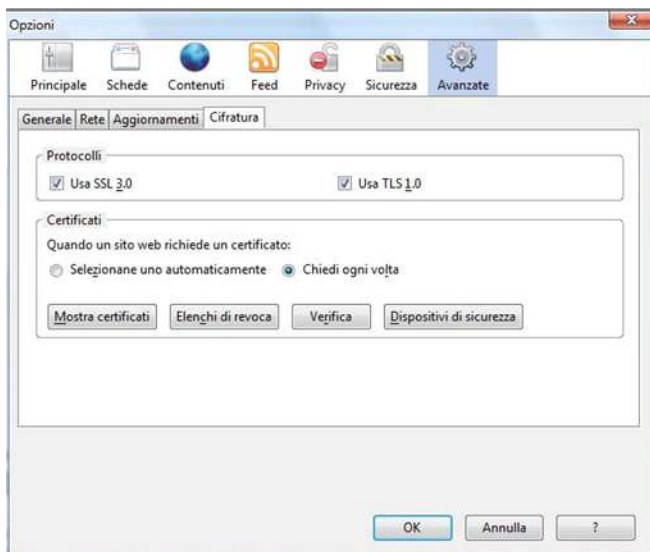
Step 9

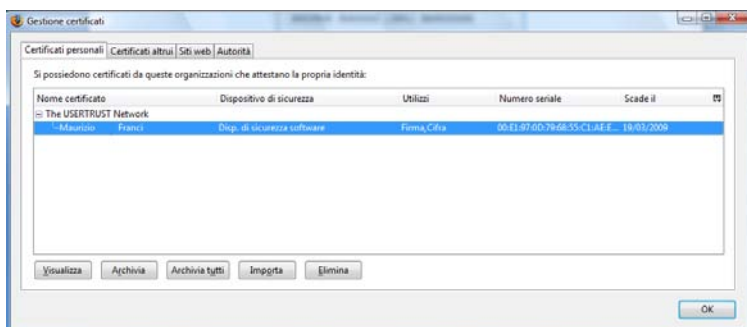
Cliccando su **Fine**, si completa la procedura di esportazione:

Il certificato di backup viene salvato nella destinazione stabilita con estensione .pfx.

Backup con Firefox 2.0.0.14

Step 1
Avviare **Firefox**

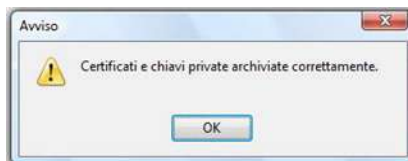
Step 2
Nella barra degli strumenti: **Strumenti →Opzioni**

Step 3

Nella sezione **Avanzate** → scheda **Cifratura** → **Mostra certificati**

Step 4

Nella sezione **Certificati personali**, si trova la lista dei certificati personali installati, selezionare il certificato che si vuole salvare in backup e cliccare su **Archivia**, avviando così la procedura di backup del certificato:

Step 5
Selezionare la destinazione e il nome del file di backup.

Step 6
Scegliere la password di protezione del certificato:

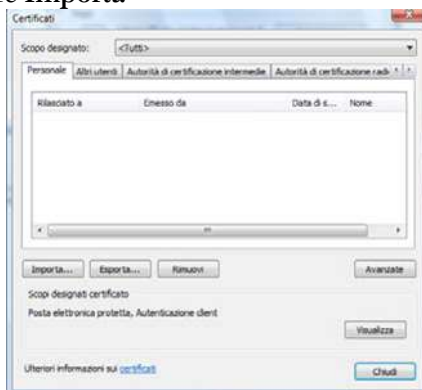
Nota: *è importante non dimenticare la password, in quanto sarà necessaria per ripristinare il certificato.*

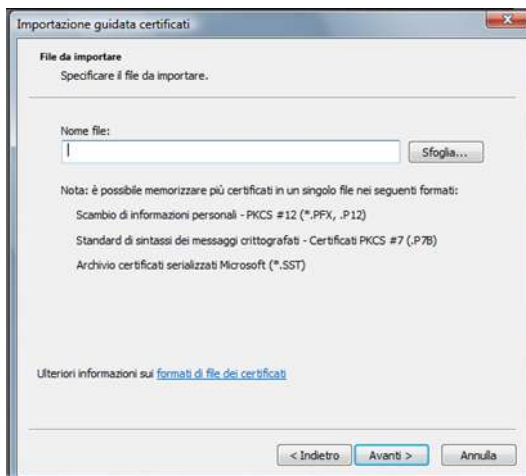
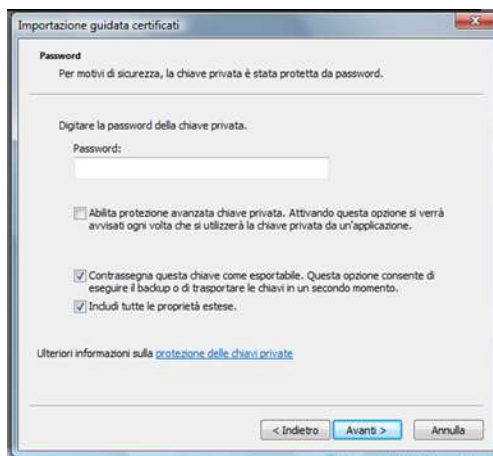
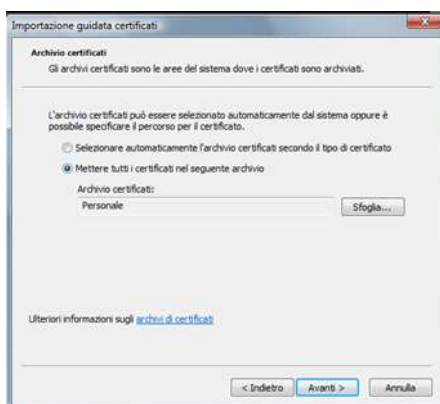
Step 7
Cliccato **OK**, compare il messaggio di avvenuta archiviazione:

Il certificato viene salvato nella destinazione prestabilita con estensione .p12.

Ripristino Certificato
In caso di perdita del certificato installato, si può in pochi click ripristinarlo grazie alla copia di backup precedentemente creata. La procedura di ripristino del certificato, prevede attraverso il browser l'operazione inversa effettuata per il backup, cioè l'**Importazione** del certificato.

Seguendo lo stesso percorso precedentemente indicato per effettuare il backup si andrà ad avviare la procedura di Importazione, che consentirà di ripristinare il certificato digitale.

Funzioni di Importazione ed esportazione dei certificati
<u>Importazione con Internet Explorer 7</u>

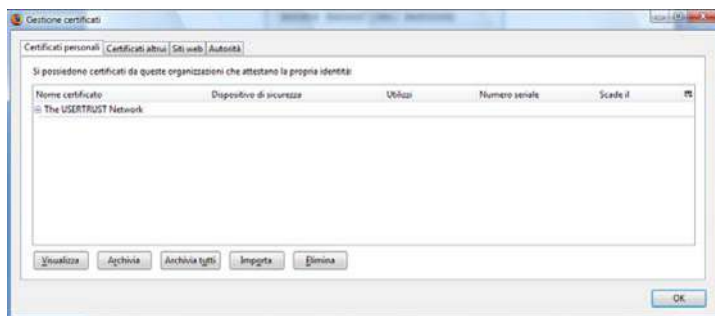
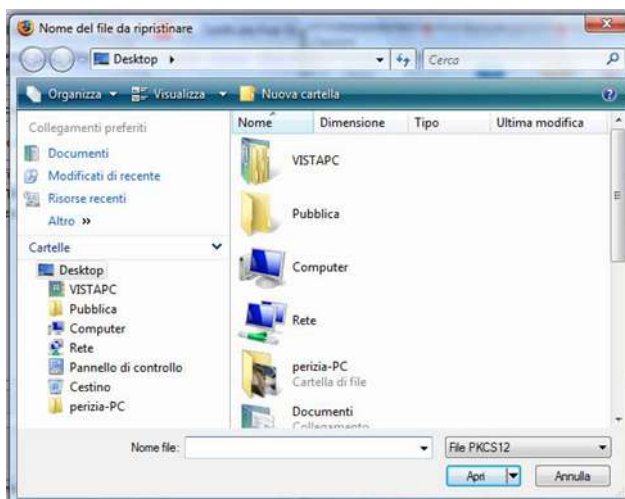
Step 1 - Cliccare **Importa**

Step 2
Cliccare **Avanti:**

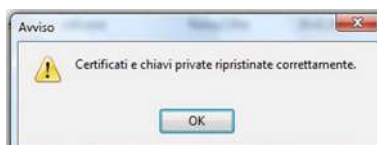
Step 3
Selezionare il certificato da importare:

Step 4
Inserire la password di protezione del certificato, stabilita al momento della creazione della copia di backup.
Attivare le opzioni: **Contrassegna questa chiave come esportabile.**
Includi tutte le proprietà estese

Step 5
Attivare l'opzione: **Mettere tutti i certificati nel seguente archivio**, in questo modo il certificato viene automaticamente installato nella sezione **Personale:**

Step 6
Cliccando **Fine** si conclude la procedura di importazione.

Completata la procedura il certificato sarà correttamente ripristinato.

Importazione con Firefox

Step 1

Cliccare **Importa:**

Step 2
Selezionare il certificato da importare:

Step 3
Inserire la password di protezione del certificato, stabilita in fase di creazione della copia di backup:

Step 4
Conferma di avvenuto ripristino del certificato:

Completata la procedura il certificato sarà correttamente ripristinato.

CONSIGLI PER AMMINISTRARE E GESTIRE I CERTIFICATI S/MIME

L'amministratore di sistema o il singolo utente, hanno la possibilità di gestire e mettere in sicurezza il certificato:

- Impedendo l'esportazione dello stesso - in questo modo il certificato non potrà essere copiato da dove è installato.
- Proteggere l'accesso e l'uso del certificato tramite password.

La combinazione delle due daranno un'adeguata sicurezza al certificato e a chi lo usa, specialmente se viene installato su un dispositivo portatile, token, smart-card o altro.

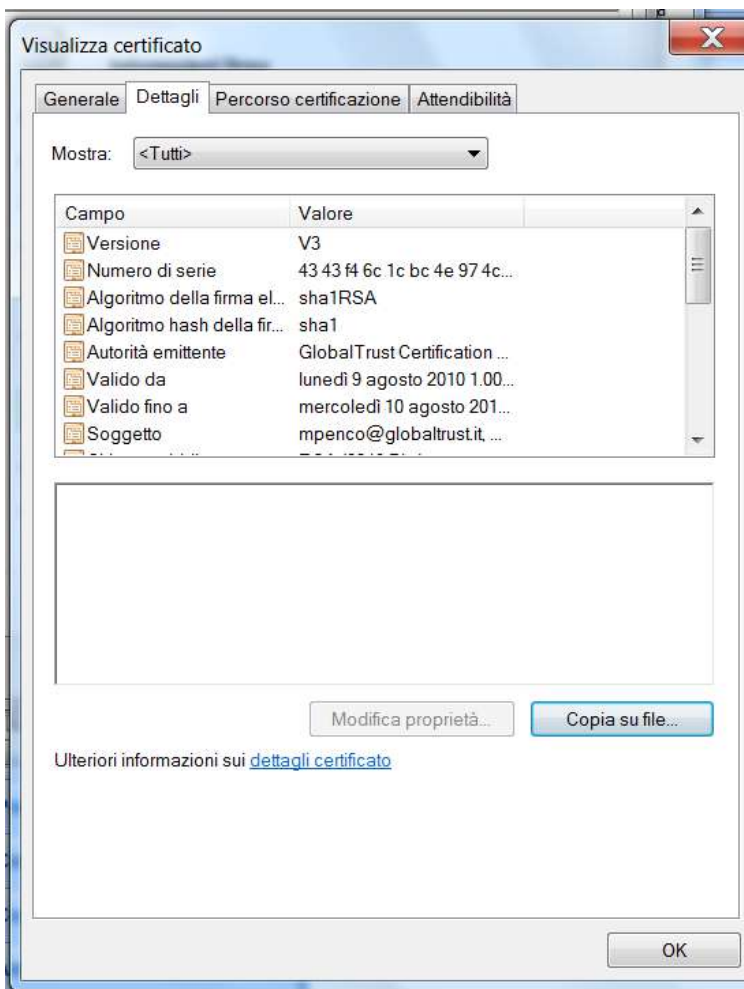
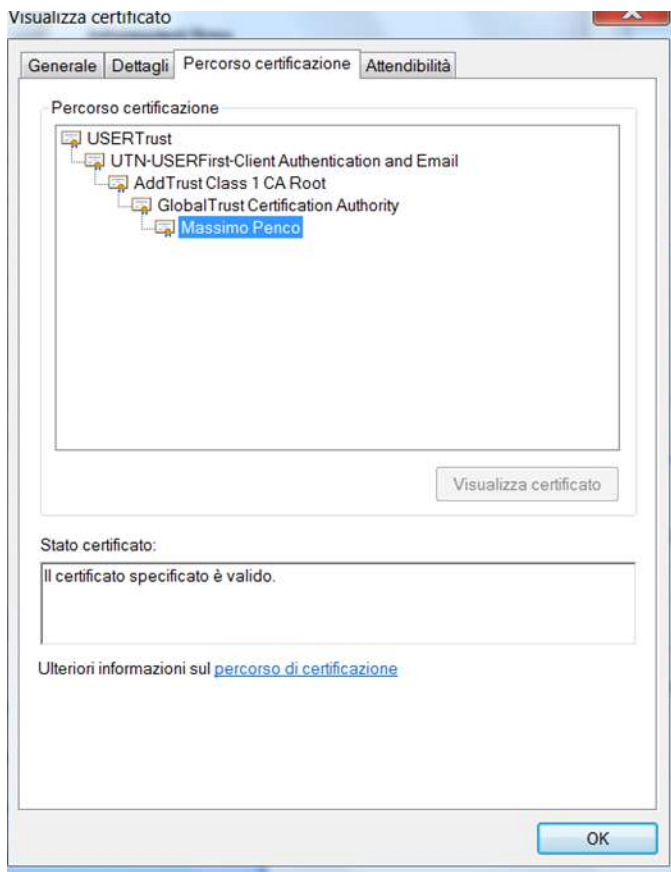
LINK per chi vuole approfondire l'argomento sull'origine ed uso del protocollo/certificato S/MIME

http://guide.debianizzati.org/index.php/Chiavi_simmetriche_e_chiavi_pubbliche
http://www.tech-faq.com/lang/it/S/Mime.shtml
http://ec.europa.eu/idabc/servlets/Doc?id=849
http://www2.cnipa.gov.it/site/_contentfiles/01379800/1379887_16%2003%2001%20caso%20aipa.pdf
http://www.microsoft.com/technet/prodtechnol/exchange/IT/Guides/E2k3ClientAccGuide/3316c76c-2527-4a78-8944-d17c075e9ab6.mspx?mfr=true
http://radarlab.disp.uniroma2.it/FilePDF/crittografia2.pdf
http://www.microsoft.com/technet/prodtechnol/exchange/IT/Guides/E2k3MsgSecGuide/02deb7c5-89d4-4e15-9300-5fc355ea83a4.mspx?mfr=true

CERTIFICATI INTERNAZIONALMENTE RICONOSCIUTI E RELATIVE CERTIFICATION AUTHORITY PUBBLICHE

Reperire la lista delle CA Internazionalmente riconosciute è molto semplice, sia le CA, che i Browser sono da tempo riuniti in un forum www.cabforum.org dove si possono trovare la lista di tutte le CA, oltre alle informazioni di base su come queste operano in tutto il mondo. Da questo contesto scaturiscono i principi di interoperabilità tra Browser e Certification Authority, ma quello che meraviglierà i lettori, non addetti ai lavori, è che la lista, per evidenti accordi

internazionali e per far si che siano funzionanti, è riconosciuta da tutti, contenuta in tutti i Browser ed apparati mobili, in cui le CA root vengono inserite nativamente non solo nei nuovi smart phone, ma anche in vecchi apparati. Vediamo i certificati ed il loro ciclo vitale:

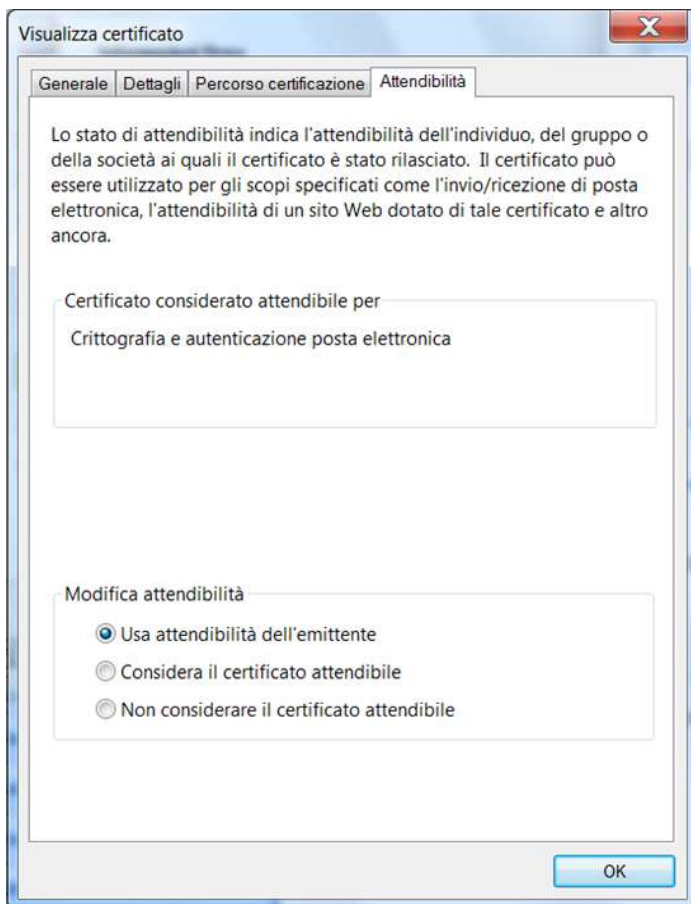
Ecco la prima schermata che appare dopo aver cliccato nella coccarda rossa del certificato che appare in ogni e-mail firmata digitalmente.

Nella schermata qui sopra si accede alla zona dettagli scorrendo la quale si hanno tutti i dettagli relativi al certificato stesso ed alle Autorità di Certificazione emittenti il certificato stesso.

Nella schermata qui sopra si accede alla zona dettagli scorrendo la quale si hanno tutti i dettagli relativi al certificato stesso ed alle Autorità di Certificazione emittenti il certificato stesso.

Il percorso di certificazione fa capire ancora meglio la correlazione tra le varie Autorità di Certificazione emittenti il certificato in quella che viene definita come " Catena di certificazione" (*Chain of Trust*), vediamo di capire un po' meglio. Ogni certificato ha bisogno di più CA per esser accettato dai browser e conseguentemente avere validità tecnica e legale in campo internazionale in poche parole non solo le Autorità di certificazione debbono certificare il titolare del certifi-

cato ma debbono anche certificarsi tra loro il complesso sistema viene definito come una infrastruttura a chiave pubblica (PKI), che viene ad essere così organizzata:

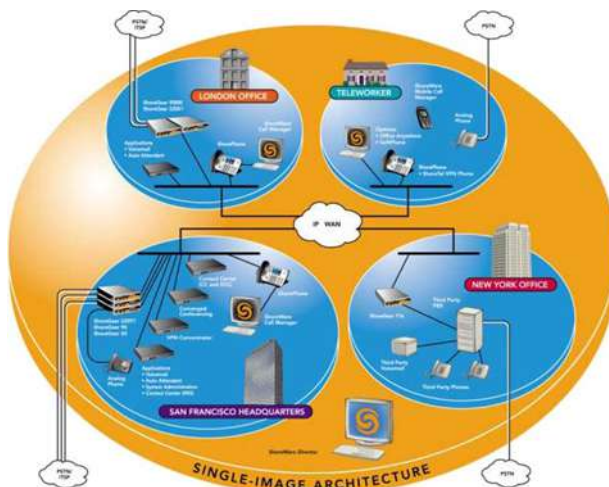
- una *policy di sicurezza* che fissa i principi generali;
- un *certificate Practice statement* (CPS), ossia il documento in cui è illustrata la procedura per l'emissione, registrazione, sospensione e revoca del certificato;
- un sistema di certification authority (CA);
- un sistema di registration authority (RA), ovvero il sistema di registrazione e autenticazione degli utenti che domandano il certificato;
- un *certificate server*.

Possono essere certificate persone fisiche, organizzazioni, server, applicazioni, ogni CA precisa nel proprio CPS chi sono le entità finali che essa è disposta a certificare e per quali scopi di utilizzo (certificati di firma e cifratura dei messaggi di posta elettronica, certificati di autenticazione dei server di rete, ecc.).

La prima nell'ordine è l'Autorità di certificazione detta radice (root CA) Una infrastruttura PKI è strutturata gerarchicamente da più CA al cui vertice si trova una CA root che certifica le sub-CA che possono essere nate specificatamente per fornire servizi specializzati questo sistema viene definito come "Certificazione Incrociata" (*crossing certification)*. Il primo passo per costruire una infrastruttura PKI è creare la CA radice dell'albero, ossia la **CA root**.
Se la CA di root è la radice dell'albero chi le firma il certificato? La risposta è molto semplice: la CA si auto firma il suo certificato. In pratica vengono create le chiavi pubblica e privata, crea la richiesta di rilascio di un certificato e la firma con la sua chiave privata, ed è per questo che sono importanti le successive CA che a loro volta certificano ad "incrocio" le altre. L'ultima è più propriamente una Registration Authority riconosciuta da tutte le CA della catena di certificazione ed incaricata di Autenticare e validare il titolare della firma od il proprietario del server.

Sembrerà strano ma in ultima analisi chi è arbitro nel considerare attendibile il messaggio di Posta elettronica firmato digitalmente è sempre ed esclusivamente il ricevente lo stesso il quale non solo sceglierà se considerare attendibile il messaggio stesso ma anche l'attendibilità dell'Autorità di certificazione.

CAPITOLO VI. 6.0
CREARE UN AMBIENTE SICURO PER LA COMUNICAZIONE AZIENDALE

Il sogno, di ogni azienda o organizzazione, è quello di creare un ambiente sicuro integrato ed interoperabile con qualsiasi altro sistema; collegare in modo planetario i propri dipendenti, collaboratori, fornitori, clienti e tutti coloro che abbiano rapporti con loro, è il "goal" che qualsiasi CTO ha in mente. Scambiare documenti, conversazioni, fare conferenze video ed audio, anche in modo protetto, rappresenta la sicura chiave di successo di qualsiasi organizzazione, in un mondo sempre più interconnesso.

Si chiama UNIFIED COMMUNICATIONS. Da alcuni anni, tutte le software house ed anche costruttori di hardware (debbo dire in modo non coordinato, come era logico, ognuno vuole mettere mano in questa importante fetta di mercato), stanno lavorando alacremente a questo progetto.
Ho scelto non per simpatia, ma per abbondanza di documentazione la soluzione MICROSOFT, rappresentata graficamente qui di seguito:

Architettura di un sistema di comunicazione unificata ed integrata.

IL CUORE DEL SISTEMA: L'AMBIENTE MICROSOFT EXCHANGE

Il cuore del sistema è basato su server Microsoft Exchange con la possibilità di interagire, tramite anche l'interfaccia OWA, con qualsiasi sistema fisso e mobile, su qualsiasi apparato e da qualsiasi posto al mondo.

INTEGRAZIONE DI TELEFONIA E POSTA ELETTRONICA

Direi che uno dei primi approcci è quello di integrare, anche ai fini dell'attrattiva riduzione dei costi, i servizi di telefonia e posta elettronica.
Vediamo l'approccio di Microsoft. Unified Communications ha una piattaforma software estendibile in grado di integrare l'infrastruttura esistente di messaggistica e voce, senza ulteriori investimenti hardware, utilizzando le soluzioni Unified Communications di Microsoft Exchange Server e di Office Outlook.

ACCESSO A TUTTI I SERVIZI DI COMUNICAZIONE, DA QUALSIASI LUOGO

Grazie a Exchange, gli utenti possono accedere in modo conveniente e sicuro a tutti i servizi di comunicazione: posta elettronica, posta vocale, messaggistica immediata e molto altro ancora, da qualsiasi piattaforma, browser Web o dispositivo, ed essere così più efficienti, ovunque si trovino. Exchange offre la miglior "esperienza utente a tre schermi" disponibile, utilizzando un computer desktop (con Outlook), il browser Web (Outlook Web App) o uno smartphone (con Exchange ActiveSync, lo standard di riferimento del settore per i dispositivi mobili). Grazie alle funzionalità integrate di Exchange ActiveSynch, è possibile ridurre i costi relativi alla messaggistica per dispositivi mobili e al contempo supportare gli utenti di qualsiasi smartphone, inclusi gli iPhone, i Windows phone o i BlackBerry.

COSTI RIDOTTI GRAZIE AL CONSOLIDAMENTO DEI SISTEMI DI TELEFONIA, POSTA VOCALE E POSTA ELETTRONICA

È possibile risparmiare tempo e denaro sostituendo i sistemi esistenti per i servizi di telefonia, posta vocale e posta elettronica, con una piattaforma Windows integrata, basata su Exchange e Office Communication Server.

È possibile semplificare la distribuzione, il provisioning e la gestione, tramite strumenti comuni, ad esempio Microsoft Active Directory, processi di distribuzione condivisi e un'unica interfaccia per l'integrità dei sistemi di report. Grazie a strumenti comuni per la gestione della sicurezza, la conformità e l'archiviazione, è possibile creare e implementare in modo più semplice, procedure dedicate ai sistemi di posta elettronica e di telefonia. Consolidando i sistemi di telefonia, posta vocale e posta elettronica, è possibile ridurre considerevolmente i costi di manutenzione e assistenza, in particolare se si tratta di uffici remoti o filiali.

Come comunicare e collaborare dalle applicazioni di Microsoft Office

Gli utenti finali non devono più chiudere Outlook o altre applicazioni per comunicare e collaborare. Possono visualizzare immediatamente la disponibilità di altri utenti in Outlook e, con un solo clic, passare da un messaggio di posta elettronica a una chiamata, o per

esempio condividere il proprio desktop. Gli utenti possono utilizzare i servizi di comunicazione in modo più rapido ed essere più produttivi perché:

- Effettuano un unico accesso a tutti i servizi di comunicazione.
- Accedono e tengono traccia di tutta la cronologia relativa alle comunicazioni, utilizzando un'unica casella di posta in arrivo.
- Utilizzano una singola interfaccia di uso comune per comunicare tramite PC, Web e Smart Device.
- Hanno un'unica esperienza utente utilizzando Outlook sul computer desktop, Outlook Web App sul browser Web ed Exchange ActiveSync, lo standard di riferimento del settore per i dispositivi mobili.

LA CREAZIONE DI UN AMBIENTE SICURO: L'INTEGRAZIONE OWA CON S/MIME E OUTLOOK

Abbiamo visto come S/MIME consente agli utenti di crittografare i messaggi e gli allegati in uscita, in modo che possano essere letti solo dai destinatari desiderati, che dispongono di un'identificazione digitale (ID), detta anche certificato.
Con S/MIME, gli utenti possono inserire la firma digitale in un messaggio, fornendo al destinatario un metodo per verificare l'identità del mittente e assicurarsi che il messaggio non sia stato alterato.
Abbiamo anche viso che l'uso di user ID e password sono da considerarsi una sicurezza debole, occorre quello che viene definito come Strong Autentication o doppio sistema di autenticazione, cioè l'istallazione, nell'area del Server WEB di Exchange, di un certificato SSL, con l'abbinamento S/Mime. Questo, darà all'infrastruttura una sicurezza assoluta in modo semplice ed economico.

Di seguito una serie di illustrazioni che indicano chiaramente come il sistema sia sicuramente predominante rispetto agli altri e possa avere diverse applicazioni in diversi ambienti.

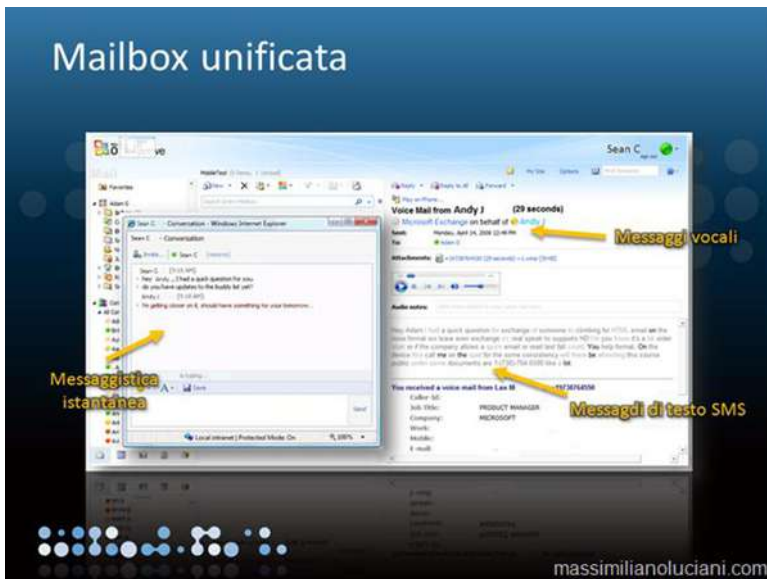
Schermata di accesso ad un sistema OWA in Microsoft E-xchange

È usato da Facebook[91] con webmail Exchange[90] via Owa[92], ovvero Outlook Web Access[93]; tanto per dare un'idea, anche visuale, rapida ed immediata della diffusione di questo sistema.
Questa è una azione piuttosto importante, per la scelta fatta, da un sistema che è praticamente un open source.
La schermata si ottiene digitando http://mail.facebook.com che punta su http://mail.thefacebook.com

Scelta praticamente obbligata, quella di Exchange, vista l'acquisizione di una parte di Facebook[94] da parte di Microsoft, avvenuta ormai qualche anno fa.

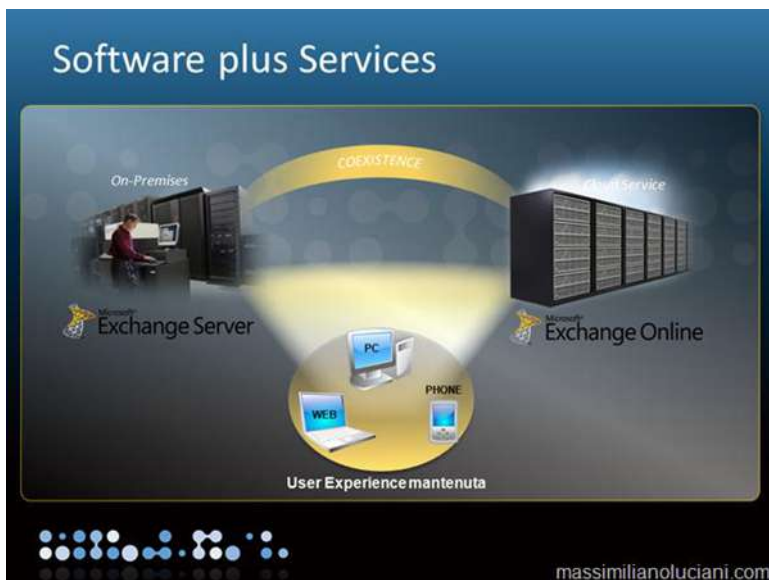
Microsoft Exchange[95] è senza dubbio uno dei software più usati in ambito aziendale. Ricordiamo, allora, alcuni tra i concorrenti come Lotus Notes[96], Zimbra[97] o Zarafa[98].

91 https://mail.thefacebook.com/owa/auth/logon.aspx?replaceCurrent=1&url=https://mail.thefacebook.com/owa/
92 http://www.domini.it/post/260/owa-webmail-outlook-web-access-per-leggere-lemail-via-web
93 http://technet.microsoft.com/it-it/library/aa998477(EXCHG.65).aspx
94 https://mail.thefacebook.com/owa/auth/logon.aspx?replaceCurrent=1&url=https://mail.thefacebook.com/owa/
95 http://www.microsoft.com/italy/server/exchange/default.mspx
96 http://www-142.ibm.com/software/products/it/it/notes/
97 http://www.zimbra.com/
98 http://www.omnis-systems.com/index.php?option=com_content&view=article&id=5&Itemid=44

LA MAILBOX DIVENTA UNIFICATA

Backbone di comunicazioni integrate dell'azienda.
Grazie al ruolo server Unified Messaging, introdotto in Exchange 2007, si ha un unico punto di immagazzinamento dei messaggi vocali, mail e fax.

Il componente Outlook Voice Access permette di interagire con il sistema utilizzando comandi vocali, è possibile ascoltare i messaggi, spostare appuntamenti, farsi leggere le mail ed i messaggi ricevuti mediante un qualsiasi telefono.

Exchange 2010 introduce delle novità, come la Voice-mail preview, il Messaging Waiting Indicator, l'integrazione con i messaggi di testo (SMS) ed un maggiore supporto per il riconoscimento vocale.

CLOUD ED ALTRE APPLICAZIONI

Microsoft, come altre organizzazioni, ha realizzato una piattaforma per ospitare servizi su cloud computing.
Exchange 2010 può essere installato on-premise (in casa), oppure, è possibile sfruttare i servizi online (cloud) di Microsoft, per ospitare le cassette postali degli utenti.
Dalla console di Exchange 2010 è possibile gestire contemporaneamente mailbox che si trovano sul cloud e quelle in casa, mantenendo la stessa *user experience* sia per gli amministratori di Exchange, che per gli utenti che non si accorgono di essere in una o nell'altra farm.

SICUREZZA E ABBINAMENTO CON S/MIME

Per supportare S/MIME nella propria organizzazione di Exchange, è necessario creare un'infrastruttura a chiave pubblica *(PKI, Public Key Infrastructure).*
Un'infrastruttura a chiave pubblica (PKI) è un sistema di certificati digitali, di Autorità di certificazione (CA) e di autorità di registrazione (RA), che verificano e autenticano la validità di ciascuna parte coinvolta in una transazione elettronica, utilizzando la crittografia a

chiave pubblica. Quando si implementa una CA, in un'organizzazione che utilizza Active Directory, si fornisce un'infrastruttura per la gestione del ciclo di vita, il rinnovo, la gestione attendibile e la revoca dei certificati. Tuttavia, la distribuzione di server e infrastrutture per creare e gestire certificati generati da un'infrastruttura a chiave pubblica di Microsoft Windows implica dei costi aggiuntivi.
È necessario che i Servizi certificati distribuiscano un'infrastruttura a chiave pubblica di Windows ed essere installati mediante Installazione applicazioni nel Pannello di controllo. È possibile installare Servizi certificati su qualsiasi server nel dominio.
Se si ottengono certificati da una CA di dominio basata su Windows, è possibile utilizzarla per richiedere o firmare certificati da emettere sui server o computer in rete. Ciò consente di utilizzare una PKI, simile all'utilizzo di un fornitore di certificati di terze parti, ma meno costosa. Poiché non è possibile distribuire pubblicamente certificati PKI, come altri tipi di certificati, quando una CA di una PKI firma il certificato del richiedente utilizzando la chiave privata, il richiedente viene verificato. La chiave pubblica di questa CA è parte del certificato. Un server, che ha questo certificato nell'archivio certificati radice attendibili, può utilizzare la chiave pubblica per decrittografare il certificato del richiedente e autenticarlo.
Una PKI consente alle organizzazioni di pubblicare i propri certificati. I client possono richiedere e ricevere i certificati da una PKI sulla rete interna. La PKI può rinnovare o revocare certificati.

REQUISITI PER IL SUPPORTO DI S/MIME IN OUTLOOK WEB ACCESS

S/MIME richiede che gli utenti eseguano l'accesso a Outlook Web App utilizzando Microsoft Internet Explorer 7 o Internet Explorer 8.
Oltre a Internet Explorer 7 o Internet Explorer 8, S/MIME richiede anche l'utilizzo di Secure Sockets Layer (SSL), da parte della directory virtuale/OWA. S/MIME non è supportato in Outlook Web App Light.

S/MIME IN OUTLOOK WEB APPLICATION

È necessario che gli utenti dispongano di un ID digitale e installino il controllo S/MIME per Outlook Web App per poter inviare messaggi crittografati e con firma digitale utilizzando OutlookWeb App.

È inoltre necessario che dispongano di un ID digitale e del controllo S/MIME, per leggere i messaggi crittografati in Outlook Web App. Il controllo S/MIME è necessario per verificare la firma in un messaggio con firma digitale.
Il controllo S/MIME per Outlook Web App viene installato nel computer di un utente tramite la scheda SMIME in Opzioni. Dopo che l'utente ha ricevuto un ID digitale e ha installato il controllo S/MIME nel computer, può utilizzare S/MIME per proteggere i messaggi di posta elettronica.

AGGIUNTE E LIMITAZIONI DI FUNZIONALITÀ CON S/MIME

Quando l'utente utilizza S/MIME, può disporre di funzionalità aggiuntive, altrimenti non disponibili in Outlook Web App.
Queste funzionalità includono la capacità di eseguire quanto segue:

- Allegare messaggi a messaggi
- Incollare immagini in messaggi
- Allegare file, utilizzando un'interfaccia utente più semplice e consentire agli utenti di allegare più file in una sola operazione.

Quando un utente utilizza S/MIME, troverà le seguenti limitazioni:

- La visualizzazione documenti WebReady funziona solo in messaggi con firma in chiaro. Non funziona nei messaggi crittografati o nei messaggi con firma nascosta.
- Quando alcuni tipi di contenuto vengono inviati da Outlook come messaggi S/MIME, non è possibile visualizzarli in Outlook Web App. Quando ciò accade, in OutlookWeb App. verrà visualizzato un banner nell'intestazione del messaggio.
- La maggior parte delle funzionalità S/MIME non è disponibile quando un utente apre una cartella in un'altra cassetta postale o utilizza l'accesso esplicito per aprire la cassetta postale di un altro utente. L'unica funzionalità S/MIME disponibile in questi casi è la verifica delle firme digitali.

CAPITOLO VII. 7.0

IL CRIMINE ATTRAVERSO LE E-MAIL

L'enorme diffusione del sistema di messaggistica tramite e-mail, ha ovviamente, provocato un interesse da parte degli hackers e di vere e proprie bande criminali su come usare questo mezzo per compiere truffe e malversazioni.

Mi limiterò a trattare brevemente tutti quei casi dove l'uso delle e-mail è predominante per l'attuazione del disegno criminoso.

Alcuni tipi di problemi ed attacchi, attraverso e-mail, il perché, le soluzioni:

- Intercettazione del messaggio (riservatezza);
- Intercettazione del messaggio (consegna bloccata);
- Intercettazione del messaggio e successiva ripetizione;
- Modifica del contenuto del messaggio;
- Modifica dell'origine del messaggio;
- Falsificazione del contenuto del messaggio da parte di terzi;
- Falsificazione dell'origine del messaggio da parte di terzi;
- Falsificazione del contenuto del messaggio da parte del destinatario;
- Falsificazione dell'origine del messaggio da parte del destinatario;
- Negazione della trasmissione del messaggio;
- Riempimento della casella di posta del destinatario.

Mentre questi sono gli attacchi insiti nella gestione della posta elettronica, quelli che seguono, sono tipici dell'uso della stessa e di comportamenti non prudenti nell'uso di Internet, in cui la posta elettronica è il mezzo per commettere crimini informatici.

L'USO DELLE E-MAIL NEL POSTO DI LAVORO

L'uso delle e-mail nel posto di lavoro non è sicuramente un crimine, ma ritengo che sia un argomento da affrontare, sia per i datori di lavoro, che per gli addetti, onde evitare spiacevoli contestazioni

dall'una e dall'altra parte. Nel testo ho riportato alcune significative sentenze sulla materia
È bene tracciare un breve modus operandi:

DA PARTE DEL DATORE DI LAVORO

a) Predisporre un completo regolamento per l'uso, non solo delle e-mail aziendali, ma anche dei Computer, dei sistemi di archiviazione dati e di tutto quello che appartiene al patrimonio informatico aziendale.
b) Evitare di immetterlo solo nella bacheca aziendale, ma allegarlo alla lettera di assunzione e farlo firmare in copia, in tutte le pagine.
c) Indicare i criteri di sicurezza informatica aziendale.
d) Nel caso di uso di sistemi di rilevazione di accesso al WEB ed al sistema di e-mail aziendale, avere cura, con l'inserimento di come interagisce il software relativo, di includerlo nel documento di cui al punto 1).
e) Non mi sento in sostanza di consigliare l'uno o l'altro testo di regolamento, è un argomento estremamente soggettivo. Per avere una visione, indico un lavoro presentato all'Università di Udine da parte del Prof. Marco Maglio[99], che dovrebbe dare un'idea della portata del documento da predisporre.

DA PARTE DEL DIPENDENTE

1. Se non si è autorizzati, non usare l'e-mail aziendale per comunicare a terzi, a mio avviso, non lo fate neanche se autorizzati, per ovvi motivi
2. La stessa cosa vale per l'uso di tutti gli apparti informatici aziendale, cellulare compreso
3. Evitare di farsi inviare messaggi di Posta elettronica all'indirizzo aziendale
4. Evitare di accedere a web-mail personale con il computer aziendale ed ovviamente a qualsiasi chat o Facebook
5. Ricordarsi sempre che tutti questi comportamenti possono essere legittimamente tracciati dall'azienda

[99] http://www.uniud.it/ateneo/organizzazione/servizi_personale/dati_personali/Uso%20degli%20strumenti%20informatici%20in%20azienda.pdf

6. Non istallare software personale, ma neanche software aziendale non munito di licenza; chiedetela è un vostro diritto.

Vi sono ovviamente numerose sentenze in materia, alcune riportate nel capitolo successivo, a volte contrastanti fra loro. Il problema è quello della conoscenza da parte dei giudici dello strumento delle e-mail e sue implicazioni. Quello che ritengo utile inserire, è senz'altro il provvedimento del Garante della protezione dei dati personali emesso nel 2007[100] che ha inteso regolare la materia, a seguito dalle numerose segnalazioni pervenute.

IL FENOMENO DELLO SPAMMING

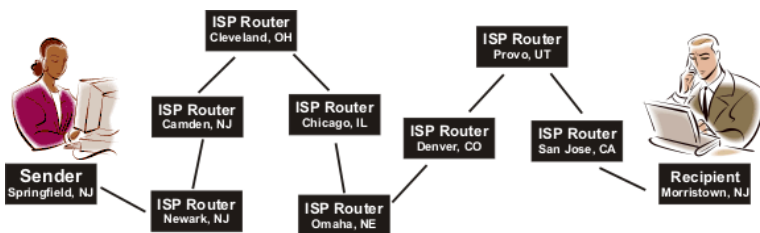
Ci si meraviglia di questo fenomeno, ma purtroppo, a volte, sono gli stessi utenti a provocarlo, navigando all'interno di siti in cui, ad esempio, fanno compilare moduli on-line non protetti da canali SSL, e non si verifica se è presente il famoso lucchettino (installando V-Engine diviene facilmente visibile). Così facendo si lascia nella rete il proprio indirizzo e-mail. Nel mondo reale e non virtuale, nessuno lascerebbe i propri dati alla portata di tutti.

Vi sono alcuni sistemi che permettono di visualizzare in modo più evidente la presenza di un certificato SSL, uno di questi è: V-Engine[101].

L'uso estensivo, da parte dei Provider o all'interno dei Server delle aziende, di filtri antispamming, è ancora più dannoso: messaggi importanti possono essere bloccati e non arrivare a destinazione. Un buon filtro antispamming personale, è molto più efficace, in quanto controllato e regolato direttamente dall'utente.

Lo schema seguente può essere d'aiuto per avere un'idea più precisa di cosa succede quando si invia un messaggio di posta elettronica:

100 http://www.garanteprivacy.it/garante/doc.jsp?ID=1387522

101 http://www.vengine.it/

Con i sistemi 'tradizionali' di trasmissione le e-mail, divengono molto simili a delle cartoline postali, il messaggio è vulnerabile e soggetto ad accessi ed utilizzi non autorizzati e quindi non sicuri visto che la trasmissione di un e-mail ed i suoi numerosi passaggi in vari sisrtemi a dir poco 'rocambolesca'.

L'immagine riportata, dimostra come un messaggio, invece di fare un semplice 'viaggio' di pochi chilometri, ne debba fare uno di circa 6000, passando attraverso numerosi ISP ed essere così esposto a molti rischi, non ultimo quello di *"sniffare"*[102] *o* *"spoofing"*[103] gli indirizzi e-mail nella rete. Esiste un vero e proprio mercato per la vendita degli indirizzi e-mail.
Si troveranno approfondimenti in:
http://www.cert.org/tech_tips/e-mail_spoofing.html
http://www.lse.ac.uk/itservices/help/spamming&spoofing.htm

FURTO DI IDENTITA'
E' una conseguenza indiretta di quanto precedentemente detto: nessuno deve rilasciare i propri dati in un'e-mail non protetta, tantomeno in un sito web non protetto.

L'identità digitale un problema irrisolto
Il tema dell'identità digitale è quanto mai attuale, alla luce di clamorosi e recenti episodi di cronaca nera e di processi giudiziari che hanno coinvolto emotivamente l'opinione pubblica. Sempre più spesso diventa determinante la "prova digitale". Si può essere assolti o condannati in base alle "tracce d'uso" di computer e telefoni cellulari, alle frequentazioni dei social network. E' allora il caso di riflettere con attenzione su come si formano queste "prove digitali" e su come vengono valutate. Insomma, l'identità digitale pesa sempre di più nella vita di ognuno di noi, ma il dibattito resta ancora negli ambiti ristretti degli addetti ai lavori. Vorrei confutare quella sorta di teorema che sembra essere ormai accettato per buono nelle aule di giustizia. Chiamiamolo, per comodità, "Teorema delle quattro P".

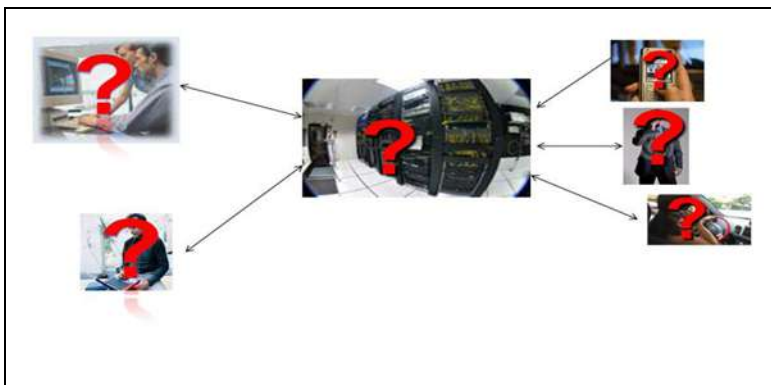
[102] http://it.wikipedia.org/wiki/Sniffing
[103] http://it.wikipedia.org/wiki/Spoofing

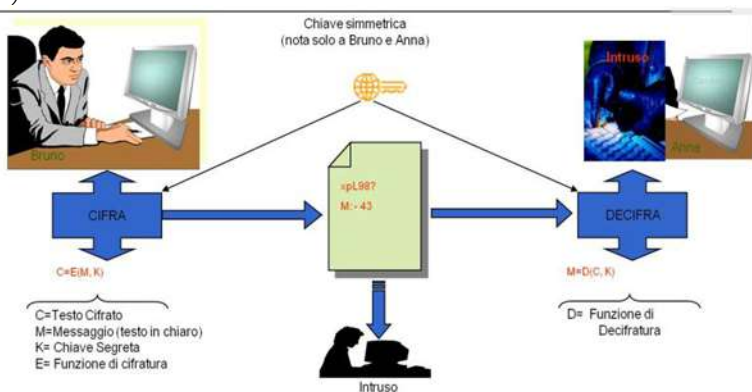
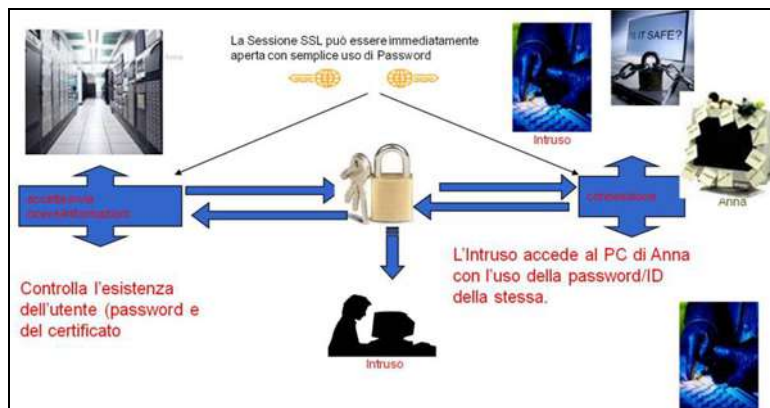
E' invalsa la consuetudine - che purtroppo è divenuta fonte di prova in alcune recenti sentenze e investigazioni, di cui la cronaca ha parlato diffusamente (caso di Garlasco e di Perugia, Scazzi, ed il rapimento di Yara) - in cui sempre di più il computer e il cellulare sono elementi primari di indagine, che evolvono in prove. La proprietà di un apparato tecnologico, PC o cellulare, fa sì che il proprietario possa sostenere e provare di aver lavorato in un certo giorno a una certa ora e, in alcuni casi (cellulare), affermare di essere in un certo posto, o essere stato localizzato nello stesso luogo.

Il teorema che la proprietà o il possesso di un oggetto sia prova di averla usata, costituiscono un'ipotesi tutta da sfatare, soprattutto nel caso in cui l'identità di chi usa l'apparato non è più fisica bensì digitale. Questo vale ancor più per gli apparati localizzabili attraverso tecnologie (GSM o GPS).

Cioè, il possesso o la proprietà di un apparato usato per comunicare non dà la certezza e la prova:

- Di chi ne fa uso;
- Del luogo fisico in cui si trova;
- Di quando lo abbia usato;
- Di quanto tempo lo abbia usato;
- In sostanza non è possibile stabilire che proprietà, possesso, uso, siano identificabili con una specifica persona fisica;
- Nessuna tecnologia è in grado di dare queste certezze;
- Gli apparati digitali, computer, cellulari, smartphone, eccetera, hanno vita e personalità autonoma, indipendentemente da chi ne ha la proprietà, li possiede e li usa.

Come vedremo, anche le più recenti ricerche tecnologiche sulla sicurezza non sono riuscite a risolvere completamente questa importante problematica e, per questo, l'identità digitale rimane un grosso problema irrisolto.
L'identità di chi opera con un computer/cellulare é nota solo a chi ne fa uso. L'operatore comunica, inserisce e riceve dati, sottoscrive digitalmente contratti, accetta clausole – interloquisce, insomma - con un'altra entità digitale, anch'essa sconosciuta.

Neanche i più moderni sistemi di trasmissione dati (Posta elettronica Certificata, certificati con firma digitale) danno la certezza di chi riceve e trasmette un messaggio di posta elettronica.

Facciamo un esempio banale, ma che evidenzia il problema.
Bruno invia un messaggio ad Anna (che ha lasciato il PC incustodito):

Davanti al PC di Anna potrebbe esserci chiunque, nonostante crittografia e firma digitale. Il certificato residente nel computer fa ritenere a Bruno che, dall'altra parte, ci sia Anna. In realtà potrebbe esserci un'altra persona che millanta l'identità della donna e dunque intercetta i dati trasmessi.
La stessa cosa accade se si usa una connessione sicura X509 (SSL), tipica dell'Home Banking: Anna lascia il PC incustodito con il proprio certificato installato.

Al posto di Anna potrebbe esserci chiunque. Il certificato residente nel computer fa sì che qualsiasi controllo del sistema non rilevi nulla di anomalo, poiché l'intruso personifica e sostituisce Anna.

Scenario analogo se si scambiano messaggi con i cellulari. Quando si riceve un SMS da un numero di cellulare noto non vuol dire che "il pollice" sia della persona che si conosce.

Non è il cellulare a stabilire "l'identità" dell'apparato, bensì la SIM, che può essere stata prelevata da un telefono e introdotta in un altro. Clonare una SIM è un gioco da ragazzi. Basta uno scanner da pochi euro.

I tecnici di tutto il mondo si basano su questi concetti cardine:

1)*something you have (qualcosa che solo tu hai)*
2)something you know (qualcosa che solo tu conosci o hai)

Sono gli assiomi della problematica dell'identità digitale. Le soluzioni fin qui adottate (user ID e password, sistemi biometrici, eccetera) non si sono dimostrate esaustive. La conoscenza del nostro user ID e password accoppiati con un dato biometrico offrono un buon livello di sicurezza, ma non assoluto.
La cinematografia ci ha proposto situazioni al limite, in cui una persona agisce sotto minaccia ed è costretta a rivelare user ID e password e, addirittura, si sottopone al controllo biometrico. Il sistema di sicurezza è così tratto in inganno dalla falsa identità digitale. Ci sono anche altri stratagemmi per bypassare la barriera biometrica.

I sistemi di difesa possono essere di due tipi:

1)Controlli a distanza;
2)Controllo accessi.

I controlli a distanza prevedono l'uso di PIN, per attivare il telefono cellulare, prelevare denaro dal bancomat, fare operazioni di Home Banking, accedere a un server via FTP, eccetera.
Il controllo accessi comprende l'ingresso in un particolare edificio, oppure la verifica del passaporto alla frontiera. Negli Stati Uniti i funzionari prelevano anche le impronte digitali e scattano una foto a chi vuole entrare nel paese.

I due sistemi hanno in comune la ricerca continua di soluzioni che rendono le procedure semplici e veloci. E' il caso dell'evoluzione dal passaporto tradizionale a quello biometrico. La direzione di marcia è la cosiddetta autenticazione multipla, basata cioè sull'acquisizione di informazione che possano essere incrociate e verificate all'istante. Con buona pace della privacy. Lo sa bene chi è andato di recente negli Stati Uniti. Innanzitutto, prima di partire, ci si deve registrare nel sito web dedicato:

All'arrivo, poi, è obbligatorio (e si pagano anche 14 dollari) farsi fotografare e sottoporsi al prelievo multiplo delle impronte digitali. C'è poi la recente introduzione (non dappertutto) del body scanner.

La banca dati del servizio di immigrazione si arricchirà dunque di queste informazioni personali:

1) Dati anagrafici completi

2) Luogo in cui si andrà a risiedere negli Stati Uniti

3) Dati Biometrici da confrontare con il passaporto elettronico

4) Foto

5) Compagnia aerea, scopo del viaggio e altro ancora.

Nel prossimo futuro (ma in alcuni casi è già realtà) è previsto:
1. lo scanning di tutto il corpo, con particolare attenzione a caratteristiche principali e eventuali malformazioni;
2. l'esame minuzioso del contenuto di ogni oggetto contenuto nella valigia imbarcata e nel bagaglio a mano
3. creazione di una cartella personale del viaggiatore, che verrà confrontata ad ogni entrata negli Stati Uniti.

Più sicurezza, meno privacy, dicono i fautori del ricorso massiccio di tecnologia per i controlli personali. E' il mondo, dopo l'11 settembre 2001, sempre più orwelliano.

PHISHING

Il phishing è un tipo di frode ideato allo scopo di rubare importanti dati personali dell'utente, ad esempio numeri di carta di credito, password, dati relativi al proprio conto bancario e così via. L'e-mail rappresenta, anche in questo caso, il mezzo naturale per perpetrare questo tipo di crimine.
Gli autori delle frodi sono in grado di inviare milioni di messaggi di posta elettronica falsi che, in apparenza, sembrano provenire da siti web sicuri, come la tua banca o la società di emissione della carta di credito, che richiedono di fornire informazioni riservate o semplicemente di interagire con un link di un sito web. Ci sono molti organismi che seguono il problema ed uno dei più importanti è l'Antiphishing Working Group, nel sito

http://www.antiphishing.org/, si potranno trovare interessanti informazioni sul fenomeno.

Che aspetto ha un messaggio di phishing?
Con l'aumentare dell'esperienza degli autori di frodi informatiche, anche i messaggi e le finestre popup, utilizzate per truffare gli utenti, diventano più sofisticati. Spesso includono il logo e altri dati di identificazione, in apparenza autentici ed effettivamente tratti dai siti Web delle aziende. Queste imitazioni sono siti Web falsificati. Una volta all'interno di uno di questi siti falsificati, è possibile che gli utenti immettano involontariamente informazioni personali, che vengono intercettate dall'autore della frode.
Come individuare i messaggi di posta elettronica fraudolenti
Di seguito vengono elencate alcune espressioni che è possibile trovare all'interno dei messaggi inviati dagli autori di una frode tramite phishing.
"La preghiamo di confermare i dati relativi al suo account."
Le aziende serie, non dovrebbero avere necessità di richiedere ai propri clienti di fornire password, dati di accesso, codice fiscale o altre informazioni tramite posta elettronica.
Se si riceve un messaggio di posta elettronica, ad esempio da Microsoft, in cui si chiede di aggiornare i dati relativi alla carta di credito, non bisogna rispondere al messaggio: si tratta sicuramente di una frode tramite phishing. Per ulteriori informazioni, leggere: Invio di messaggi di posta elettronica fraudolenti che richiedono i dati della carta di credito ai clienti Microsoft[104].
"Se non riceveremo risposta entro 48 ore, il suo account verrà chiuso."
Questi messaggi sottolineano spesso l'urgenza della risposta per indurre ad agire senza soffermarsi a pensare. I messaggi di posta elettronica con phishing attuano tale procedura sostenendo che, in mancanza di una risposta, potrebbero verificarsi dei problemi con l'account.
"Gentile cliente."
I messaggi contraffatti vengono solitamente inviati in blocco a diversi destinatari e non contengono il nome o cognome dei singoli utenti.

[104] http://www.microsoft.com/italy/athome/security/email/msphishing.mspx

"Fare clic sul collegamento sottostante per accedere al proprio account."
www.truffa.it
All'interno dei messaggi in formato HTML è possibile inserire collegamenti o moduli compilabili in modo analogo a quelli presenti nei siti Web. I collegamenti che vengono chiesti di utilizzare possono contenere tutto o parte del nome di un'azienda autentica e sono solitamente "mascherati", ovvero il collegamento visualizzato, non corrisponde all'indirizzo reale, ma rimanda ad un altro sito Web, solitamente predisposto dall'autore della frode.
Di seguito è riportato un esempio dell'aspetto di un messaggio di posta elettronica utilizzato per il phishing.

C'è una molteplicità di software che "cerca" di determinare la reale provenienza di un sito Web ed anche delle e-mail di phishing. E'

stimabile un vecchio progetto “Calling ID Link Advisor” elaborato dal Prof. Yoram Nissenboim dell’Università di Haifa (che per un lungo periodo ho cercato di rendere noto in Italia senza molto successo), a mio avviso molto semplice e valido, ma soprattutto utile a far capire il problema e la metodologia per risolverlo.

In questo caso l’uso di “Calling ID Link Advisor” permette di conoscere a chi appartiene il link, normalmente inviato con un’e-mail, prima di cliccarci.
I due prodotti collegati fra loro ***Calling ID*** e ***Link Advisor*** permettono, una volta installati, di conoscere a chi appartiene un sito Web, la proprietà del link inviato con un’e-mail prima di cliccarci sopra. Purtroppo il prodotto funziona solo con Explorer ed alcune versioni di Firefox ed è interessante vederlo in azione www.callingid.com (è gratuito).
Utilizza un algoritmo in grado di eseguire 54 test di verifica delle pagine web. Se il sito non supera tutto o in parte la verifica, *CallingID* informa l’utente del “*rischio in corso*”, se è il caso o meno di procedere con la navigazione e/o inviare le proprie informazioni personali (es. username, password, numero della carta di credito, etc.).I risultati dei test vengono riassunti e visualizzati in un toolbar che si avvale di 3 indicatori di facile intuizione che informano e aiutano l’utente durante la navigazione.
Di seguito gli schemi di funzionamento e specifiche tecniche:

LOW RISK - Ci sono dei problemi, il sito non ha superato completamente i test di verifica.

VERIFIED - In questo caso è sicuro navigare all’interno del sito Web.

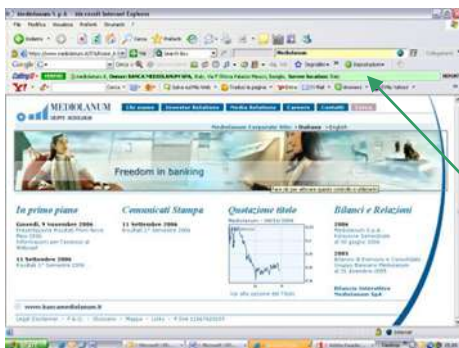
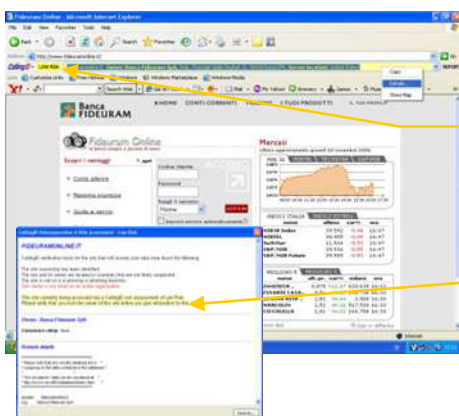
HIGH RISK - Se compare questo indicatore. Navigare e/o fornire informazioni è molto rischioso!

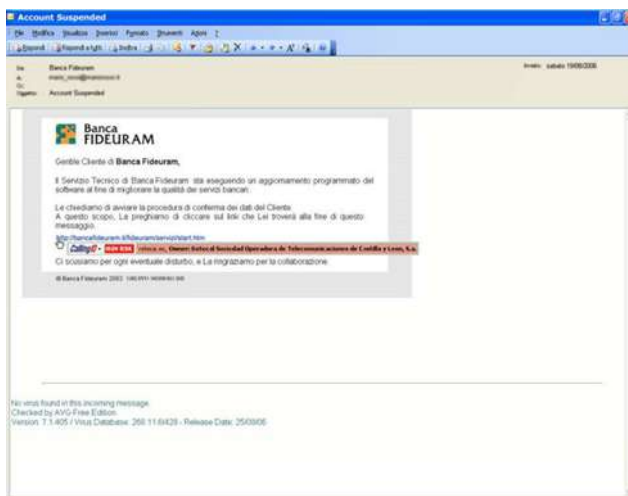
HIGH RISK **Phishing!!.**
Il dominio non corrisponde e non appartiene al reale proprietario del sito!.

HIGH RISK **Phishing!!.**
Si attiva una finestra che invita a non inviare dati personali in quanto il sito è altamente pericoloso!!.

LOW RISK
C'è qualcosa che non va!
È meglio controllare più approfonditamente!
Se si clicca con il tasto destro del mouse sulla banda gialla, compare un menu a tendina.
Scegliendo "Details" avremo la possibilità di vedere i risultati dei test che Calling ID ha effettuato nel sito in questione:

- chi è il proprietario del dominio;
- dove è situato il server che ospita il sito,etc.

In questo caso viene segnalato che il nome del dominio non è un'organizzazione attiva e non corrisponde al nome della società che lo ha registrato.

VERIFIED **OK!!**
Il sito ha superato i test di verifica!
Non solo!
La "doppia" presenza del lucchetto nella barra verde di *CallingID* e nella barra di stato del browser, da l'assoluta tranquillità ad acquistare e fornire i propri dati personali all'interno del sito in questione!

- **Perché cliccare su un link che arriva all'interno di un'e-mail?!?**

Controlla automaticamente i link che vengono ricevuti nelle e-mail, *Instant Messenger*, o anche all'interno di una pagina web prima che vengano cliccati, verificando le credenziali e la loro attendibilità. Ciò permette di conoscere ancora prima di iniziare a navigare a chi appartiene il sito WEB.

- Perché non conoscere preventivamente tutti i link presenti in una pagina WEB?

Esplora automaticamente i siti che si intendono visitare e fornisce tutte le informazioni in tempo reale! Segnalando con i colori della barra i siti pericolosi o meno.

CYBER-STALKING

Il fenomeno dello Stalking è relativamente nuovo, in special modo per la giustizia Italiana, che solo recentemente lo ha inquadrato come reato. Uno dei mezzi usati dagli Stalker è senz'altro l'e-mail, oltre ad altro tipo di messaggistica come SMS, telefono, fax, social network ed altro ancora.

È importante notare come, ancora una volta, non ci sia un preciso indirizzo tecnico giuridico in materia. Difatti, una recente sentenza della Cassazione, anche se non riferente propriamente al reato di stalking, ha dato un'interpretazione del tutto singolare, con sentenza che riporto per intero a pag. 202.

La Suprema Corte stabilisce che la molestia via e-mail non e' perseguibile di per sé, così come avviene per una telefonata o un sms. Il messaggio ingiurioso pervenuto tramite posta elettronica non comporta, a differenza della telefonata, nessuna immediata interazione con il soggetto interessato, la modalità della comunicazione via mail, si osserva nella sentenza, è "asincrona" e "l'invio di un messaggio di posta elettronica, esattamente proprio come una lettera spedita tramite il servizio postale, non comporta, a differenza della telefonata,

alcuna immediata interazione tra il mittente e il destinatario, né intrusione diretta del primo nella sfera delle attività del secondo".
Decisione questa che merita un minimo di commento, come sempre accade quando giudici, giuristi, cercano di capire come funziona un sistema come quello delle e-mail senza dialogare fra loro. Ho detto più volte in questo libro e del resto, non è solo la mia opinione, ma anche quella di decine di studiosi in materia, che, se l'e-mail non è inviata in sicurezza è come la cartolina postale (e-mail is like postcard); una metafora largamente usata, per la quale si sono scritti interi volumi[105].
Voglio riportare quanto scritto da **Hossein Bidgoli** nella sua "**The Internet Encyclopedia**" pag. 524, dove è chiaramente illustrato il concetto della metafora E-mail = cartolina postale. Ora, se minimamente ci si fosse soffermati su questo concetto, molto probabilmente questa sentenza non ci sarebbe stata. È evidente a tutti, che un'e-mail inviata su Internet può essere letta da chiunque, con le conseguenze ben immaginabili in casi simili e nei casi di stalking, del resto, uno dei motivi per cui la nostra polizia postale, una volta allertata, riesce ad arrivare con molta facilità al colpevole, è dovuto al fatto che lo stalker si comporta in modo sciocco, inviando per l'appunto messaggi in chiaro, che vengono con molta facilità intercettati con tutto il contenuto anche dall'autorità inquirente (un famoso caso è riportato in: Bidgoli, H. (2009). *The Internet.* John Wiley & Sons, Inc.). Anche il sistema per risalire con molta facilità allo stesso, è portare le relative prove in tribunale, certo che se poi si arriva a sentenze come queste, il lavoro fatto viene ad essere inutile. Una meravigliosa chiara esposizione che lascio in lingua originale per non far perdere il senso lucido e pracmatico.

[105] **Hossein Bidgoli** is a tenured professor at California State University Bakersfield in the Management Information System department within the school of Business. Professor Bidgoli is a two-time winner of Meritorious Performance and Professional Promise Award for 1985-86 and 1988-89, School of Business and Public Administration, California State University, Bakersfield, these awards were granted based upon outstanding performance in teaching, research and school/community service. Professor Bidgoli is also the recipient of the outstanding professor (professor of the year) award for 2001-2002. Professor Bidgoli is the author or editor of 41 books, numerous peer-reviewed articles and a trainer and consultant.

Postcards versus Letters versus E-Mail

It is a widely used metaphor that unprotected e-mail is like a postcard in the physical postal system, not like a letter. There is no envelope protecting the content of the message. This is why we need security; we expect messages to have some degree of privacy and integrity to them.

However, like all metaphors, this can be stretched until it breaks. Although e-mail resembles postal mail in many ways, it is not postal mail and there is no direct correspondence of the components of an e-mail to that of a letter.

Not only is there no envelope that wraps an e-mail, but the address portions of each do not exactly correspond. (There is also no stamp on an e-mail, as some people have observed in spam fighting and this is what makes the problem of junk e-mail much worse than of junk mail, even if that is merely degree and not kind.) This means that although the postal system offers metaphors and analogies to e-mail systems designers, we simply cannot graft systems from the past onto those in the present.

CAPITOLO VIII. 8.0
COME SCRIVERE UNA BUONA E-MAIL

In questo libro non potevano mancare alcuni brevi consigli su come scrivere una buona e-mail. Ovviamente ci sono interi trattati su questo argomento da leggere e consultare, e qui ci si limita a dare alcune regole basilari che possono essere utili.

LA POSTA ELETTRONICA È UNA GRANDE OPPORTUNITÀ

La posta elettronica è oggi il mezzo più veloce ed economico per comunicare. Non solo con un singolo soggetto, ma anche con tante persone in una volta sola. È sufficiente una mailing list, un clic e il messaggio parte per il mondo in tante direzioni arrivando a destinazione in pochi minuti.
La tentazione di inondare il prossimo con missive è forte. Però, proprio perché riceviamo tante e-mail, la tendenza a cestinarle ancor prima di aprirle cresce in proporzione al numero dei messaggi in arrivo. Non fa certo piacere leggere nell'avviso di ritorno *"il messaggio è stato cancellato senza essere letto"*.
La lettura sullo schermo non aiuta, i messaggi appaiono tutti uguali, il linguaggio è spesso sciatto e troppo colloquiale. Un "Salve Anna" seguito da un testo, che chiaramente, viene inviato tale e quale ad altre migliaia di persone in tutto il mondo, ci sembra quasi una presa in giro.
Un clic e l'e-mail prende la strada del cestino. Superata questa prima problematica, magari mettendo nell'oggetto qualcosa che colpirà od incuriosirà il destinatario, si passa al testo.

QUELLO CHE CONTA, COME IN UNA CONVERSAZIONE, SONO LE PAROLE

Quando scrivete un'e-mail le parole sono la forza e l'unica risorsa; non potete ricorrere a carta patinata, a colori appariscenti, al logo dell'azienda, alle animazioni, che ormai ammiccano da ogni pagina web. Anche se nelle moderne e-mail si potrebbe inserire tutta una serie di elementi grafici ed anche sonori, il problema rimane. L'e-mail deve essere prima aperta, è quel clic che deve essere superato. Una volta ottenuto questo, si hanno solo le parole per farsi leggere,

per incuriosire, interessare e ottenere una risposta. Quindi si deve imparare a usarle e disporle bene.

L'oggetto è un'esca

Come detto prima, se volete che l'e-mail venga almeno aperta, cosa non così scontata, prima ancora di mettersi a scrivere, si deve dedicare la massima attenzione alla riga *oggetto/subject*. Non si deve mai ometterla, ma condensare in quei pochi caratteri il contenuto del messaggio. L'oggetto deve essere breve, esplicito e il più possibile preciso. Non "novità", ma quale novità. Non "sito Internet", ma "aggiornamenti sito x". Non "nuova offerta clienti", ma " Internet Banking".

Non è il telegramma di una volta ma brevi, anzi brevissimi messaggi

La brevità, sempre raccomandabile, per un'e-mail è d'obbligo. Tutto quello che si ha da dire deve assolutamente stare nella prima schermata, addirittura nelle prime righe. Nessuno ha più voglia e tempo di scorrere fino alla trentesima riga per sapere quello che si intende comunicare. Quindi, preparate prima una piccola scaletta, mettendo gli argomenti in ordine di priorità. Se avete bisogno di più spazio, iniziate il messaggio con un piccolo indice, preferibilmente numerato, magari con la tecnica dell'indice ipertesto, così il destinatario può andare direttamente all'argomento che lo interessa. Se il vostro interlocutore è particolarmente interessato al punto 6, saprà subito dove andare a cercare con un semplice clic.

Impaginazione

La vostra e-mail deve essere densa solo di informazioni e contenuti, ma quasi rarefatta dal punto di vista visivo. Una schermata piena di parole tutte uguali, senza stacchi, è destinata a scoraggiare chiunque. È vero, non avete molte risorse, ma quelle che avete usatele bene. Quindi:

1. indice iniziale, se il documento è lungo;
2. paragrafi molto brevi, introdotti da titoletti maiuscoli (evitare corsivo e neretto, non tutti li leggono);
3. spazio bianco tra un paragrafo e l'altro;
4. uso di liste, puntate o numerate, per condensare e rendere meglio visibili le informazioni;

5. righe corte, di 70 caratteri al massimo;
6. ricordare che molto spesso le vostre e-mail vanno a finire in un palmare in cui non sono visibili grafici o fiorellini.

Formale, ma non troppo

Non lasciatevi tentare a tutti i costi dalle formalità o al contrario dall'informalità della posta elettronica: il segreto è una via di mezzo. Un "ciao, tutto ok" va benissimo, se si scrive ad un amico o ad un collaboratore. Se invece si contatta un cliente o un fornitore e si presenta un progetto, bisogna ricordare che il sito Internet dell'azienda è stato appena aggiornato, mantenete un tono colloquiale, ma al tempo stesso professionale. Non si deve esordire con un "caro cliente!, la ditta X presenta una straordinaria offerta" e poi compilare il testo come se si parlasse. Si deve progettare l'e-mail così come si farebbe per qualsiasi altro documento verso il mondo esterno.

A ciascuno il suo linguaggio e la forma relativa

Trovar,e quindi, il tono giusto e usare un linguaggio semplice e asciutto, calibrare il linguaggio su quello dell'interlocutore. Non scrivere al cliente come se fosse un amico, ma non cominciare nemmeno con un classico "ci pregiamo informarLa", né concludere con un "In attesa di un Suo gentile riscontro, cogliamo l'occasione per inviarLe i nostri migliori saluti". All'inizio "Vogliamo informarla sulla nostra offerta di ……." e alla fine "Cordiali saluti" vanno benissimo. E anche il Lei o il Voi con la maiuscola non si addicono all'e-mail.

L'e-mail che si clicca

Introdurre nel testo del messaggio un briciolo di **interattività**, per esempio dei **link** alle pagine aggiornate del proprio sito Internet o ad altri siti di interesse: il colore o carattere diverso già attira l'occhio e pochi resistono alla tentazione del clic. Utilizzare, inoltre, i link per non appesantire il messaggio: se si vuole informare i clienti su un nuovo prodotto, si deve invitarli ad andare direttamente sul sito a scaricare la brochure; con tutti i colori, l'impaginazione e gli effetti giusti, non allegare megabyte di informazioni, si potrebbe intasare la casella del destinatario.

Anche la firma parla del mittente

Utilizzare al meglio la firma. Non solo il nome e cognome (rigorosamente senza dott. o ing.), ma anche l'azienda, la struttura a cui si appartiene, l'e-mail, il telefono, il fax, l'indirizzo, l'url del sito Internet o quella dell'azienda (preferibilmente cliccabile). Confezionare diverse firme da inserire automaticamente: informale, formale, in italiano, in inglese.

Prima di inviare

Una volta finito di scrivere il testo, non cliccare automaticamente sul pulsante Invio, consigliabile salvarlo prima. Anche l'e-mail ha bisogno di editing e di revisione. Un'e-mail con refusi ed errori non depone certo a favore dell'accuratezza e affidabilità del mittente. Rileggere tutto con attenzione, controllare l'impaginazione, aprire gli allegati per controllare che siano quelli giusti, verificare l'indirizzo e i destinatari se sono più d'uno. E solo allora inviare il messaggio.

CAPITOLO IX. 9.0
LA NORMATIVA IN ITALIA

La normativa italiana sulla PEC[106]

La normativa principale contenente disposizioni relative anche indirettamente alla PEC, comprese le principali circolari del CNIPA (ora DigitPA), è presente nel Codice dell'Amministrazione digitale, mentre già è stata annunciata alla stampa (19.02.2010) l'approvazione da parte del Consiglio dei Ministri di un nuovo Codice dell'Amministrazio-ne Digitale, è oggi: D.L. 193 del 29 dicembre 2009 (pubblicato sulla G.U. n. 302 del 30.12.2009 e convertito in Legge ordinaria dall'art. 1 comma 10 della L. 22 febbraio 2010 n. 24) "*Interventi urgenti in materia di funzionalità del sistema giudiziario*";

- D.Lgs. 1 dicembre 2009, n. 177. "*Riorganizzazione del Centro nazionale per l'informatica nella pubblica amministrazione, a norma dell'articolo 24 della legge 18 giugno 2009, n. 69*";
- D.P.C.M. 6 maggio 2009. "*Disposizioni in materia di rilascio e di uso della casella di posta elettronica certificata assegnata ai cittadini*";
- D. L. 29-11-2008 n. 185. "*Misure urgenti per il sostegno a famiglie, lavoro, occupazione e impresa e per ridisegnare in funzione anti-crisi il quadro strategico nazionale*" (Convertito con L. 28 gennaio 2009, n. 2, pubblicato nella Gazz. Uff. 29 novembre 2008, n. 280);
- D.P.R. 11 febbraio 2005, n. 68. "*Regolamento recante disposizioni per l'utilizzo della posta elettronica certificata, a norma dell'articolo 27 della L. 16 gennaio 2003, n. 3*";
- D.Lgs. 7 marzo 2005, n. 82. "*Codice dell'amministrazione digitale*";
- D.M. 2 novembre 2005. "*Regole tecniche per la formazione, la trasmissione e la validazione, anche temporale, della posta elettronica certificata*";
    - CENTRO NAZIONALE PER L'INFORMATICA NELLA PUBBLICA AMMINISTRAZIONE: CIRCOLARE n. 56 del 21 maggio 2009.

"*Modalità per la presentazione della domanda di iscrizione nell'elenco pubblico dei gestori di posta elettronica certificata (PEC) di cui all'articolo 14 del decreto*

[106] Tratto d al Libro L a P EC Posta E lettronica Cer tificata d i E milio Ro botti **COLLANA I NFORMATICA GIURIDICA** diretta da Michele Iaselli edita da Altalex

del Presidente della Repubblica 11 febbraio 2005, n. 68"; CIRCOLARE 7 dicembre 2006, n. 51.

"*Espletamento della vigilanza e del controllo sulle attività esercitate dagli iscritti nell'elenco dei gestori di posta elettronica certificata (PEC),di cui all'articolo 14 del decreto del Presidente della Repubblica 11 febbraio 2005, n. 68, «Regolamento recante disposizioni per l'utilizzo della posta elettronica certificata, a norma dell'articolo 27 della legge 16 gennaio 2003, n. 3»*" (abrogata dalla Circ. 56/2009).

L'utilizzo della PEC tra privati e tra questi e le P.A., tra le P.A.
L'utilizzo della PEC nei rapporti tra privati e/o tra questi e la P.A. è disciplinato già nel Codice dell'Amministrazione Digitale e nel D.P.R. N.68/2005. Quest'ultimo prevede all'art. 4 (utilizzo della posta elettronica certificata), che la trasmissione dei messaggi di posta elettronica certificata è efficace agli effetti di legge e, per quanto riguarda i privati, che l'unico indirizzo(PEC) valido, ad ogni effetto giuridico, è quello espressamente dichiarato ai fini di ciascun procedimento con le pubbliche amministrazioni, o relativamente ad ogni singolo rapporto intrattenuto tra privati, o tra questi e le pubbliche amministrazioni.
Inoltre, secondo la norma suddetta, la dichiarazione dell'indirizzo di posta elettronica certificata obbliga solo il dichiarante e può essere revocata nella stessa forma, mentre la volontà di indicare un indirizzo PEC per tali rapporti, sorta di elezione di domicilio telematico, non può essere desunta dalla mera indicazione dell'indirizzo di posta certificata nella corrispondenza (ad esempio, tipicamente nella carta intestata del soggetto), o dalla sua indicazione in altre comunicazioni o pubblicazioni del soggetto interessato.
Va detto, per completezza, che il D.M. 2 novembre 2005 consente che la dichiarazione dell'indirizzo PEC, anche nei casi di variazione dell'indirizzo di posta elettronica certificata o di cessazione della volontà di avvalersi della posta elettronica certificata medesima, possa essere resa anche mediante l'utilizzo di strumenti informatici; ma in tal caso essa deve essere sottoscritta con la firma digitale di cui all'art. 1, comma 1, lettera n) del decreto del Presidente della Repubblica n. 445 del 2000. Se l'utilizzo della PEC tra privati è quindi rimesso ad una dichiarazione esplicita del soggetto, che intenda avvalersi di tale mezzo di comunicazione, con indicazione del proprio

indirizzo PEC per quello specifico rapporto, lasciando completamente alla volontà delle parti, la scelta anche in modo asimmetrico tra loro sull'utilizzo o meno della PEC, differente (o almeno dovrebbe essere) è invece la situazione per quanto riguarda il rapporto tra Pubbliche amministrazioni, tra di esse ed il cittadino.
Già nel Codice dell'Amministrazione Digitale (D.Lgs. 7 marzo 2005, n. 82), si prevede (art.47 "***Trasmissione dei documenti attraverso la posta elettronica tra le pubbliche amministrazioni"***) che le comunicazioni di documenti tra le pubbliche amministrazioni, debbano avvenire, di norma, mediante l'utilizzo della posta elettronica, e che esse siano valide, ai fini del procedimento amministrativo, una volta che ne sia verificata la provenienza da parte della P.A. Ai fini di tale verifica dell'accertamento della provenienza delle comunicazioni così inviate tra le pubbliche amministrazioni, sono positive secondo il Codice, se:

a) sono sottoscritte con firma digitale o altro tipo di firma elettronica qualificata, ovvero
b) se sono dotate di protocollo informatizzato, o ancora se
c) è comunque possibile accertarne altrimenti la provenienza, secondo quanto previsto dalla normativa vigente o dalle regole tecniche di cui all'articolo 71 del Codice, o infine, se
d) sono trasmesse attraverso sistemi di posta elettronica certificata di cui al decreto del Presidente della Repubblica 11 febbraio 2005, n. 68.

Sempre secondo l'articolo 48 del Codice, entro otto mesi dalla data della sua entrata in vigore le pubbliche amministrazioni centrali provvedono (o meglio, avrebbero dovuto provvedere) a istituire almeno una casella di posta elettronica istituzionale ed una casella di posta elettronica certificata ai sensi del decreto del Presidente della Repubblica 11 febbraio 2005, n. 68, per ciascun registro di protocollo; inoltre le P.A. sono tenute ad utilizzare la posta elettronica per le comunicazioni tra loro ed i propri dipendenti, nel rispetto delle norme in materia di protezione dei dati personali e previa informativa agli interessati in merito al grado di riservatezza degli strumenti utilizzati. Ulteriormente, il comma 6 dell'art. 16-bis del decreto-legge 29 novembre 2008, n. 185, prevede che ogni amministrazione pubblica utilizzi unicamente la posta elettronica certificata con effetto equivalente, ove necessario, alla notificazione per mezzo della posta,

per le comunicazioni e le notificazioni aventi come destinatari dipendenti della stessa o di altra amministrazione pubblica. Oltre a ciò, l'art. 48 del Codice, prevede che la trasmissione telematica di comunicazioni necessitanti di una ricevuta di invio e di una ricevuta di consegna, debba avvenire mediante la posta elettronica certificata, che la trasmissione del documento informatico per via telematica, effettuata mediante la posta elettronica certificata, equivalga, nei casi consentiti dalla legge, alla notificazione per mezzo della posta, ed ancora, che la data e l'ora di trasmissione e di ricezione di un documento informatico, trasmesso mediante posta elettronica certificata, siano opponibili ai terzi, se conformi alle disposizioni di cui al decreto del Presidente della Repubblica 11 febbraio 2005, n. 68, ed alle relative regole tecniche.
Ancora, il D.P.C.M. 6 maggio 2009 all'art. 4. (Modalità di attivazione della PEC per le pubbliche amministrazioni) conferma quanto previsto dal Codice dell'Amministrazione Digitale, relativamente all'obbligo delle pubbliche amministrazioni, di cui all'art. 1, comma 2 del decreto legislativo 30 marzo 2001, n. 165, di istituire una casella di PEC per ogni registro di protocollo e darne comunicazione al CNIPA (ora DigitPA), che provvede alla pubblicazione in rete consultabile per via telematica; stabilisce che le pubbliche amministrazioni devono inoltre rendere disponibili sul loro sito istituzionale, per ciascun procedimento, ogni tipo di informazione idonea a consentire l'inoltro di istanze da parte dei cittadini titolari di PEC, tra le quali in particolare l'indicazione dei tempi previsti per l'espletamento della procedura, ed accettare le istanze dei cittadini inviate tramite PEC nel rispetto dell'art. 65, comma 1, lettera c), del decreto legislativo n. 82 del 2005.
Infine, ma non per importanza, come vedremo anche più oltre, significativa e rilevante è la previsione normativa che l'invio tramite PEC costituisca sottoscrizione elettronica ai sensi dell'art. 21, comma 1, del decreto legislativo n. 82 del 2005, ma è d'obbligo precisare che le pubbliche amministrazioni possono comunque richiedere all'instante la sottoscrizione mediante firma digitale, ai sensi dell'art. 65, comma 2, del citato decreto legislativo.

Istanze alla P. A. tramite: PEC e firma digitale

A rigore, si potrebbe forse pensare che sia assolutamente necessario, per presentare un'istanza per via telematica alla Pubblica Ammini-

strazione tramite PEC, proporla sotto forma di file di testo, firmato con la firma digitale dell'istante, come allegato ad un messaggio PEC dalla casella dell'istante a quella della P.A. destinataria; almeno se si tiene presente che le istanze cartacee devono essere sottoscritte dall'istante nel momento della presentazione, o anche precedentemente se trasmesse per fax o via telematica, ma allegando fotocopia di un documento di identità ai sensi dell'art. 38 D. Lgs. 445/2000).
In realtà la risposta a tale domanda è data dall'art. 4 del DPCM 6.5.2009, il quale dispone che l'invio tramite PEC costituisce sottoscrizione elettronica ai sensi dell'art. 21, comma 1, del D.Lgs. 82/2005, e che le P.A. accettano le istanze dei cittadini presentate attraverso la PEC (o la CEC-PAC).
Ciò ha provocato (giustificatamente) lo sconcerto di vari commentatori (ad es. il già citato A. Lisi e G. Penzo Doria " *Che PEC-cato! La posta elettronica certificata tra equivoci e limitati utilizzi* concreti" in ALTALEX - http://www.altalex.com/index.php?idnot=49104) di fronte ai continui mutamenti normativi, ed al fondato sospetto che il legislatore si muova in senso scomposto, forse non sempre comprendendo appieno gli strumenti sui quali legifera, in questo caso la PEC; ma soprattutto ciò ha fatto ritenere ad alcuni che la firma digitale sulle istanze telematiche dei cittadini alle P.A. sia destinata a diventare qualcosa di residuale o addirittura a scomparire. In realtà, non è detto che sia affatto così, come osserva G. Rognetta, in ALTALEX - "*La PEC come firma elettronica nella gestione dei flussi documentali*" in **http://www.altalex.com/index.php?idnot=4926**

a) la firma digitale rimane, nell'ambito della gestione informatica dei flussi documentali, il superiore contrassegno di autenticità, per nulla scalfito dalla configurazione della PEC come firma elettronica (non qualificata). Nella disciplina generale della trasmissione telematica alle pubbliche amministrazioni di istanze e dichiarazioni, il D.Lgs. 82/2005 si affida alla firma digitale quale strumento che può essere configurato come indispensabile nei casi necessari: infatti, l'art. 65, comma 2, stabilisce che le pubbliche amministrazioni possano stabilire quando è necessaria la sottoscrizione con firma digitale. Le cautele di una corretta gestione dei flussi documentali, anzi, impongono alle pubbliche amministrazioni di effettuare tale valutazione ai fini della conseguente scelta: si configura, quindi, una deroga al generale principio di possibilità di utilizzo della sola PEC (o della carta

nazionale servizi o, ancora, della carta di identità elettronica). La predetta disposizione è ribadita dall'art. 4, comma 4, del DPCM 6.5.2009, secondo cui le pubbliche amministrazioni devono sì accettare l'invio, da parte dei cittadini, di istanze tramite PEC (o CEC-PAC), ma non per questo esse sono private del potere di richiedere anche la sottoscrizione con firma digitale (ove lo ritengano, appunto, necessario).

b) L'invio di un'istanza tramite PEC (senza firma digitale ove non escluso dall'amministrazione destinataria) sarà inquadrato, dal ricevente/gestore del flusso documentale, come firma elettronica non qualificata, la cui efficacia probatoria deriverà dalle sue caratteristiche oggettive di qualità, sicurezza, integrità e immodificabilità (art. 21, comma 1, CAD)."

ALCUNE IMPORTANTI SENTENZE

Ci sono molte sentenze relative alle e-mail e si è cercato di raccogliere le più significative elencando i link per le altre a pag. 213

05.07.10 - Cassazione Civile: la molestia via posta elettronica non è molestia

(Corte di Cassazione – Prima Sezione Penale, Sentenza 30 giugno 2010, n.24510: Molestie via posta elettronica - Esclusione contravvenione)

"**La avvertita esigenza di espandere la tutela del bene protetto (della tranquillità della persona) incontra il limite coessenziale della legge penale costituito dal "principio di stretta legalità" e di tipizzazione delle condotte illecite, sanciti dall'articolo 25, comma 2, della Costituzione e dall'articolo 1 del Codice Penale". Con questa conclusiva motivazione la Cassazione ha annullato senza rinvio la sentenza impugnata perché il fatto non è previsto dalla legge come reato. Nel caso di specie si trattava della contravvenzione di molestia alle persone per aver inviato con la posta elettronica un messaggio recante apprezzamenti gravemente lesivi della dignità e della integrità personale e professionale del convivente della destinataria**.

La Cassazione ha rilevato che "nel concorso colla causa di estinzione del reato prevale, tuttavia, quella assolutoria ai termini dell'articolo 129, comma 2, C.P.P. Giova premettere che il giudice a quo ha

definitivamente prosciolto il giudicabile dal contestato delitto di ingiuria (capo sub C della rubrica, concorrente ai sensi dell'articolo 81, comma l, del Codice Penale colla contravvenzione in esame), perché l'azione penale non doveva essere iniziata per mancanza di querela. Orbene risulta evidente ex actis che il fatto - per quanto concerne la residua ipotesi contravvenzionale - non è previsto a legge come reato.

La questione è stata, invero, affrontata dal giudice di merito. Il Tribunale ha considerato: "la tipizzazione della condotta incriminata dall'articolo 660 Codice Penale, non risulta tassativamente espressa nel dettato normativo; si tratta di indicazione aperta [..] legata all'evolversi dei mezzi tecnologici disponibili, colla conseguenza che l'aumento della "gamma delle opportunità intrusive", offerto dal progresso tecnologico, si correla alla espansione dell'ambito delle "condotte in grado di integrare l'elemento strutturale della molestia" e del "corrispondente livello di tutela apprestato alle potenziali vittime", restando " inalterata la ratio della norma incriminatrice; in tal senso la giurisprudenza di legittimità ha ravvisato gli estremi della contravvenzione nella condotta molestatrice attuata col mezzo del citofono, sulla base del rilievo che l'articolo 660 Codice Penale colla dizione "telefono" comprende gli "altri analoghi mezzi i comunicazione a distanza"; e, comunque, anche "la e-mail viene propriamente inoltrata col mezzo del telefono"".

Tuttavia, secondo la Cassazione "La tesi del giudice di merito (peraltro apprezzabilmente argomentata) non è condivisibile. Il tribunale è incorso nella erronea applicazione della legge penale. La quaestio juris è se la interpretazione estensiva della previsione della norma incriminatrice, circa la molestia o il disturbo recati "col mezzo del telefono", possa essere dilatata sino a comprendere l'invio di corrispondenza elettronica sgradita, che provochi turbamento o, quanto meno, fastidio. Innanzitutto non coglie nel segno l'argomento del giudice di rito secondo il quale la "e-mail [..] viene propriamente inoltrata col mezzo del telefono" così integrando la previsione della norma incriminatrice. Il rilievo è improprio e inesatto. La posta elettronica utilizza la rete telefonica e la rete cellulare delle bande di frequenza ma non il telefono, né costituisce applicazione della telefonia

che consiste, invece nella teletrasmissione in modalità sincrona, di voci o di suoni. Né poi, giova il richiamo al precedente di questa Corte suprema relativo alla molestia citofonica, citato dal Tribunale … In relazione all'oggetto giuridico della norma incriminatrice l'azione perturbatrice dei due sistemi di telecomunicazione vocale (telefono e citofono) è perfettamente identica; le differenze tecniche tra telefonia e citofonia sono, sotto tale aspetto assolutamente irrilevanti; e deve, pertanto, ribadirsi la interpretazione estensiva della disposizione penale".

Infatti "**Notevolmente diversa è, invece, la comunicazione effettuata con lo strumento della posta elettronica. La modalità della comunicazione è asincrona. L'azione del mittente si esaurisce nella memorizzazione di un documento di testo (colla possibilità di allegare immagini, suoni o sequenze audiovisive) in una determinata locazione dalla memoria del collaboratore del gestore del servizio, accessibile dal destinatario; mentre la comunicazione si perfeziona, se e quando il destinatario, connettendosi, a sua volta, all'elaboratore e accedendo al servizio, attivi una sessione di consultazione della propria casella di posta elettronica e proceda alla lettura del messaggio**.
In tutta evidenza è l'analogia con la tradizionale corrispondenza epistolare in forma cartacea, inviata, recapitata e depositata nella cassetta (o casella) della posta sistemata presso l'abitazione del destinatario". Secondo la Cassazione " **l'invio di un messaggio di posta elettronica - esattamente proprio come una lettera spedita tramite il servizio postale - non comporta (a differenza della telefonata) nessuna immediata interazione tra il mittente e il destinatario, né veruna intrusione diretta del primo nella sfera delle attività del secondo.**

Orbene, l'evento immateriale - o psichico - del turbamento del soggetto passivo costituisce condizione necessaria ma non sufficiente infatti per integrare la contravvenzione prevista e punita dall'articolo 660 Codice Penale, devono concorrere (alternativamente) gli ulteriori elementi circostanziali della condotta del soggetto attivo, tipizzati dalla norma incriminatrice: la pubblicità (o l'apertura al pubblico) del teatro dell'azione ovvero l'utilizzazione del telefono come mezzo del reato. E il

mezzo telefonico assume rilievo - ai fini dell'ampliamento della tutela penale altrimenti limitata alle molestie arrecate in luogo pubblico o aperto al pubblico - proprio per il carattere i intrusivo della comunicazione alla quale il destinatario non può sottrarsi, se non disattivando l'apparecchio telefonico, con conseguente lesione, in tale evenienza, della propria libertà di comunicazione, costituzionalmente garantita (articolo 15, comma 1, Costituzione). Tutto esclude la possibilità della interpretazione estensiva seguita dal Tribunale.

Soccorre, infine, anche la considerazione delle ragioni che hanno indotto questa Corte a risolvere positivamente la questione della inclusione nella previsione della norma incriminatrice dei messaggi di testo telefonici (Sez. III, 26 giugno 2004, n. 28680, Modena, massima n. 229464: "La disposizione di cui all'articolo 660 Codice Penale punisce la molestia connessa col mezzo del telefono, e quindi anche la molestia posta in essere attraverso l'invio di short messages system (SMS) trasmessi attraverso sistemi telefonici mobili o fissi".

SUPREMA CORTE DI CASSAZIONE - SEZIONE V PENALE
Sentenza 14 dicembre 2007, n. 46674

Svolgimento del processo
...*omissis*...
Con l'impugnata sentenza è stata confermata la dichiarazione di colpevolezza di A. M. A. in ordine al reato p. e p. dagli artt. 81, 494 c.p., contestatogli "perché, al fine di procurarsi un vantaggio e di recare un danno ad A. T., creava un account di posta elettronica, ********@libero.it., apparentemente intestato a costei, e successivamente, utilizzandolo, allacciava rapporti con utenti della rete Internet al nome della A.T., e così induceva in errore sia il gestore del sito sia gli utenti, attribuendosi il falso nome della A.T.".
Ricorre per cassazione il difensore deducendo violazione di legge per l'erronea applicazione dell'art. 494 c.p. e per la mancata applicazione dell'art. 129 c.p.p..
Lamenta che non siano state confutate dalla corte fiorentina le critiche rivolte al convincimento di colpevolezza espresso dal primo

giudice siccome basato sulla duplice errata considerazione, inerente la prima alla tutela di stampo civilistico al nome e allo pseudonimo, l'altra, più propriamente tecnico-informatica, alla sostenuta necessità di fornire all'ente gestore del servizio telefonico l'esatta indicazione anagrafica al momento della richiesta di fornitura della prestazione telematica.

Tali doglianze non possono essere condivise.

Oggetto della tutela penale, in relazione al delitto preveduto nell'art. 494 c.p.,è l'interesse riguardante la pubblica fede, in quanto questa può essere sorpresa da inganni relativi alla vera essenza di una persona o alla sua identità o ai suoi attributi sociali. E siccome si tratta di inganni che possono superare la ristretta cerchia d'un determinato destinatario, così il legislatore ha ravvisato in essi una costante insidia alla fede pubblica, e non soltanto alla fede privata e alla tutela civilistica del diritto al nome.

In questa prospettiva, è evidente la configurazione, nel caso concreto, di tutti gli elementi costitutivi della contestata fattispecie delittuosa.

Il ricorrente disserta in ordine alla possibilità per chiunque di attivare un "account" di posta elettronica recante un nominativo diverso dal proprio, anche di fantasia. Ciò è vero, pacificamente.

Ma deve ritenersi che il punto del processo che ne occupa sia tutt'altro.

Infatti il ricorso non considera adeguatamente che, consumandosi il reato "de quo" con la produzione dell'evento conseguente all'uso dei mezzi indicati nella disposizione incriminatrice, vale a dire con l'induzione di taluno in errore, nel caso in esame il soggetto indotto in errore non è tanto l'ente fornitore del servizio di posta elettronica, quanto piuttosto gli utenti della rete, i quali, ritenendo di interloquire con una determinata persona (la A.T.), in realtà inconsapevolmente si sono trovati ad avere a che fare con una persona diversa.

E non vale obiettare che "il contatto non avviene sull'intuitus personae, ma con riferimento alle prospettate attitudini dell'inserzionista", dal momento che non è affatto indifferente, per l'interlocutore, che "il rapporto descritto nel messaggio" sia offerto da un soggetto diverso da quello che appare offrirlo, per di più di sesso diverso.

È appena il caso di aggiungere, per rispondere ad altra, peraltro fugace, contestazione difensiva, che l'imputazione ex art. 494 c.p.p.

debitamente menziona pure il fine di recare - con la sostituzione di persona - un danno al soggetto leso: danno poi in effetti, in tutta evidenza concretizzato, nella specie, come il capo B) della rubrica (relativo al reato di diffamazione, peraltro poi estinto per remissione della querela) nitidamente delinea nella subdola inclusione della persona offesa in una corrispondenza idonea a ledere l'immagine o la dignità (sottolinea la sentenza impugnata che la A.T., a seguito dell'iniziativa assunta dall'imputato, "si ricevette telefonate da uomini che le chiedevano incontri a scopo sessuale").
Il ricorso va pertanto respinto, con le conseguenze di legge.
P.Q.M.
La Corte rigetta il ricorso e condanna il ricorrente al pagamento delle spese del procedimento.
<u>Legittimo il Controllo della Posta Elettronica del Dipendente</u>

A tale conclusione sono giunti il giudice del lavoro e quello penale, chiamati a valutare se l'indagine in questione è compatibile con l'articolo 616 del codice penale e con l'articolo 4 dello Statuto dei lavoratori.

L'articolo 616 del codice penale punisce (tra l'altro) «... chiunque prende cognizione del contenuto di una corrispondenza chiusa, a lui non diretta, ovvero sottrae o distrae, a fine di prenderne o di farne da altri prendere cognizione, una corrispondenza chiusa o aperta, a lui non diretta ...».
Come specificato al comma 4, in materia di delitti contro la inviolabilità dei segreti, per corrispondenza si intende, tra l'altro, quella informatica o telematica.
L'articolo 4 della legge 20 maggio 1970, n. 300 modera i vincoli (in materia di controlli a distanza sull'attività del lavoratore) alla discrezionalità del datore di lavoro, per consentirgli l'esercizio del suo potere direttivo e di garantire la sicurezza delle condizioni di lavoro.
Oltre alla presenza di queste esigenze è però necessario, perché possa essere parzialmente sacrificata la riservatezza del dipendente, che l'installazione della strumentazione (con cui si può effettuare il controllo sulla sua attività) sia concordata con il sindacato.
Infatti l'articolo 4, che vieta «... l'uso di impianti audiovisivi e di altre apparecchiature per finalità di controllo a distanza dell'attività dei

lavoratori ...», ne consente però l'installazione «....quando siano richiesti da esigenze organizzative e produttive ovvero dalla sicurezza del lavoro, previo accordo con le rappresentanze sindacali aziendali, oppure in mancanza di queste, con la commissione interna ... ».
Solo nel caso in cui si sia tentato di raggiungere un accordo senza successo, si può supplire alla mancata intesa chiedendo l'autorizzazione all'installazione alla Direzione provinciale del lavoro. Appare opportuno soffermarsi sulla particolare vicenda in esame, che ha originato i due giudizi.

Durante l'assenza dal lavoro di una dipendente, il diretto superiore (che, peraltro, ne aveva chiesto il trasferimento per non essere riuscito a stabilire con lei un rapporto di. adeguata collaborazione) ha acceso il computer assegnato alla medesima e individuato, nella corrispondenza elettronica della lavoratrice, delle e-mail inviate, su richiesta del precedente superiore, a quest'ultimo (in precedenza trasferito ad altro incarico nell'ambito della stessa azienda).
Si trattava di e-mail recanti documentazione lavorativa e tabulati, a disposizione della dipendente in ragione delle sue mansioni.

Secondo il giudice del licenziamento (Tribunale di Vasto, sentenza dell'11 aprile 2005) la condotta della ricorrente non integra una grave negazione dell'elemento fiduciario proprio del rapporto di lavoro. In particolare non integra una inosservanza dell'obbligo di segretezza assoluta sugli interessi dell'azienda (previsto dal con tratto nazionale applicabile alla ricorrente) anche perché l'ex superiore (della lavoratrice), per la propria nuova posizione lavorativa, avrebbe comunque potuto chiedere legittimamente accesso a quanto inviatogli per posta elettronica dalla ex collaboratrice.
Il giudice, d'altro lato, ha ritenuto che l'accesso al computer ed alla posta elettronica del lavoratore non violi l'articolo 4 della legge 20 maggio 1970, n. 300 (Statuto dei lavoratori), che riguarderebbe «... esclusivamente l'uso di apparecchiature per il controllo a distanza e così non suscettibile di applicazione analogica (siccome anche penalmente rilevante ai sensi già dell'arti colo 38 dello Statuto dei Lavora tori e ad oggi, degli articoli 114 e 171 del Decreto legislativo n. 196/2003 (codice in materia protezione dei dati personali)...».
Il giudice penale è stato invece adito per la assenta violazione dell'articolo 616 del codice penale.

La sentenza di rigetto (del 15 settembre 2006) de Tribunale di Torino - sezione distaccata di Chivasso - si basa sulla considerazione che i messaggi inviati dal dipendente, attraverso la e-mail dell'impresa, costituiscono corrispondenza aziendale e non del lavoratore.
La motivazione rimarca che **i computer dell'azienda devono essere equiparati agli altri strumenti lavorativi a disposizione dei dipendenti**.
Circostanza dimostrata, nella vicenda in esame, dalla menzione nell'indirizzo di posta elettronica dell'identificativo dell'azienda e dalla possibilità, per il servizio informatico della medesima, di accedere ai computer aziendali.
Più in generale si ricorda che la norma in esame, in effetti, tutela non il segreto eventualmente affidato alla corrispondenza, ma la corrispondenza in sé, che è considerata di per sé stessa segreta a prescindere dal suo con tenuto.
In dottrina si è pure avanzata l'ipotesi dell'inapplicabilità del divieto di cognizione di corrispondenza chiusa (di cui alla norma in esame) alla corrispondenza elettronica, che sarebbe in vece aperta.
Ma di contro si è osservato che anche la lettura delle e-mail richiede l'apertura delle medesime, sia pure attraverso una semplice operazione del mouse.
Inoltre si ritiene tutelata dalla predetta norma esclusivamente la corrispondenza «in movimento» dal mittente al destinatario, vale a dire quella che il destinatario non ha ancora aperto (se si tratta di corrispondenza chiusa) o della quale non abbia ancora preso visione (nel caso in cui si tratti di corrispondenza aperta).
La corrispondenza già aperta e letta è invece tutelata dalla normativa in tema di furto e di appropriazione indebita.

I precedenti giurisprudenziali

Mentre in materia di controlli a distanza sui collegamenti alla rete, Internet aziendale, le sentenze più recenti sono di segno favorevole al lavoratore, una panoramica sulla scarna giurisprudenza in tema di controlli sulla posta elettronica, evidenzia, solamente, un'importante pronuncia del Tribunale di Milano, sfavorevole al dipendente.
Secondo l'ordinanza del 10 maggio 2002 non integra gli estremi del reato di violazione della corrispondenza, di cui all'articolo 616, comma 1, Codice penale il datore di lavoro che controlli la casella di

posta elettronica del dipendente a sua insaputa (nel caso in esame il lavoratore si trovava in ferie), perché questi non è titolare di un diritto all'utilizzo esclusivo della posta elettronica aziendale e, conseguentemente, si espone al rischio che altri lavoratori o il datore di lavoro possano lecitamente entrare nella sua casella e leggere i messaggi.
Infatti, secondo questa ordinanza «... il lavoratore che utilizza - per qualunque fine - la casella di posta elettronica aziendale, si espone al "rischio" che anche altri lavoratori della medesima azienda - che, unica, deve considerarsi titolare dell'indirizzo - possano lecitamente entrare nella sua casella (ossia in suo uso sebbene non esclusivo) e leggere i messaggi (in entrata e in uscita) ivi contenuti, previa consentita acquisizione della relativa password la cui finalità non è certo quella di «proteggere» la segretezza dei dati personali contenuti negli strumenti a disposizione del singolo lavoratore bensì solo quella di impedire che ai predetti strumenti possano accedere persone estranee alla società».
Dunque non si può confondere la personalità dell'e-mail aziendale - in quanto legata alla persona del dipendente che ne è titolare - con il concetto di «privatezza» della casella di posta elettronica.

Il datore di lavoro mette a disposizione del dipendente, per consentirgli di svolgere al meglio la propria attività, **un'e-mail che però rimane nella completa disponibilità dell'azienda**.
Inoltre, anche volendo ignorare i rilievi sull'elemento oggettivo del reato in questione, secondo detta sentenza, in ogni caso la fattispecie di cui all'articolo 616 non può considerarsi integrata per la mancanza dell'elemento del dolo, visto che l'accesso alla casella di posta elettronica era avvenuto per motivi assolutamente connessi allo svolgimento dell'attività aziendale.
Interessante, anche se relativa ad una diversa fattispecie, la sentenza del Tribunale Amministrativo del Lazio, n. 9425 del 15 novembre 2001.
In questo caso l'amministrazione convenuta in giudizio non ha controllato la casella di posta elettronica del dipendente, ma ha avuto direttamente accesso al testo di un'e-mail inviata dal lavoratore (un diplomatico) al circuito privato «Diplomazia», recante critiche all'operato del Ministero degli Esteri, che aveva portato ad una formale nota di deplorazione da parte del direttore del personale. Se-

condo la sentenza (favorevole al dipendente) la posta elettronica «... deve essere tutelata alla stregua della corrispondenza epistolare o telefonica ed è quindi caratterizzata dalla segretezza...».

La normativa a tutela della privacy

La predetta, recente, sentenza del Tribunale di Torino si produce in un azzardato richiamo al principi affermati dal Garante per la Protezione dei Dati Personali: «il lavoratore - secondo quanto indicato dal Garante per la privacy nel proprio parere del 16 giugno 1999, poteva invocare il diritto alla riservatezza fino a quando il datore di lavoro non avesse chiarito formalmente, mettendolo nero su bianco, che tutti i testi in entrata e in uscita da qualsiasi account interno all'azienda potevano essere resi pubblici in qualsiasi momento». In realtà quella che la sentenza definisce interpretazione autentica del Garante della privacy, è di segno diverso.

Con parere del 16 giugno 1999, l'Authority ha affermato che la posta elettronica rientra nella corrispondenza protetta dall'articolo 15 della Costituzione e nella tutela approntata (dagli articoli 615, 618 e seguenti del codice penale) in favore della corrispondenza epistolare e telefonica.

In questa ottica le norme che tutelano la riservatezza della corrispondenza si applicano anche in ambito aziendale e, a prescindere da chi sia il proprietario dei mezzi utilizzati per effettuare corrispondenza e comunicazioni, si ha diritto a mantenerle segrete.

Va considerato pure il parere del 12 luglio 1999, con il quale il Garante della privacy ha asserito che «la legge n. 547/1993 sui reati informatici e, da ultimo, il Decreto del Presidente della repubblica n. 513/1997 sul documento elettronico, hanno confermato poi che la posta elettronica deve essere tutelata alla stregua della corrispondenza epistolare o telefonica (si veda anche l'arti colo 616, comma 4 del codice penale, come sostituito dall'articolo 5 della legge n. 547, e l'articolo 13 del Decreto del Presidente della Repubblica n. 513, che parlano di corrispondenza «informatica o telematica»).

Per le caratteristiche avute sinora dalla rete ..., i messaggi che vi circolano vanno quindi considerati alla stregua della corrispondenza privata ...». In un comunicato del 7 luglio 2001 il Garante ha rimar-

cato che in materia è applicabile l'art. 4 dello Statuto dei lavoratori, che non consente alcun controllo a distanza sull'attività del lavoratore, se non dopo accordo sindacale e definizione di precisi limiti per l'impresa.
Non si può, inoltre, trascurare la portata più generale in cui si colloca il diritto al riservatezza della posta elettronica.
Come rilevato da Stefano Rodotà, in relazione alle norme costituzionali, «... la libertà della comunicazione elettronica, fondata sul rispetto delle informazioni personali, condiziona la libertà di associazione (art. 18) visto che molti gruppi si formano ormai at traverso la rete; e incide sulle manifestazioni del pensiero (art. 21), se Internet diviene un luogo sottoposto ad un controllo continuo e generalizzato». (La Repubblica, pagina 16, del 5 marzo 2 004).
Passando agli ultimi mesi, secondo quanto rilevato dal presidente dell'Autorità, Francesco Pizzetti (su La Stampa dello scorso 13 ottobre):
«La corrispondenza elettronica personale del dipendente è inviolabile, è un diritto costituzionale. E se in pochi casi un dirigente deve entrare nella casella elettronica di un collaboratore, deve solo leggere ciò che serve all'azienda, null'altro. E comunque questi casi andrebbero previsti in una direttiva nota a tutti i dipendenti».
Mentre all'estero la questione è stata risolta con l'uso di due e-mail, una professionale l'altra personale ma in Italia è difficile affrontare il tema, anche perché i sindacati non collaborano.

Dunque, secondo il Garante per la Protezione dei Dati Personali i controlli sulla posta elettronica sono ammissibili, esclusivamente, se previsti in relazione a un numero circoscritto di casi e con riferimento alle e-mail che abbiano un contenuto legato all'attività aziendale.
Sono più di una le norme del codice in materia di protezione dei dati personali che non possono essere trascurate, in materia di controlli sull'attività del lavoratore.
In primo luogo l'articolo 13, alla stregua del quale l'azienda deve fornire all'interessato un'informativa relativa al trattamento dei dati sul suo conto prima di effettuarlo.
Inoltre l'articolo 11 impone di trattare i dati in modo lecito e secondo correttezza, nel rispetto dei principi di pertinenza e non eccedenza rispetto alle finalità perseguite.

Bisogna pure ricordare il principio di necessità (di cui all'artico- lo 3 del codice), che impone di configurare i sistemi informativi e i programmi informatici riducendo al minimo l'utilizzazione di dati personali e di dati identificativi.
D'altro lato l'articolo 24, primo comma, lettera f) esclude l'obbligo di informativa e consenso dell'interessato quando il trattamento sia necessario per far valere o difendere un diritto in sede giudiziaria, ma appare molto discutibile la riconduzione a detta norma dell'intrusione nella posta elettronica del lavoratore, che può in effetti potenzialmente risolversi con un licenziamento impugnato per via giudiziale.
Nel caso esaminato dalla predetta pronuncia del Tribunale di Torino, quantomeno appare assolto l'obbligo di comunicare ai dipendenti la possibilità di controlli sull'utilizzo della posta elettronica.
Infatti, come rimarcato dalla succitata sentenza penale, disposizioni aziendali espressamente precisavano che:
«La strumentazione informatica e quanto con essa creato è di proprietà aziendale in quanto mezzo di lavoro. E' pertanto fatto divieto di utilizzo del mezzo informatico e delle trasmissioni interne ed esterne con esso effettuate per fini ed interessi non strettamente coincidenti con quelli della Società e con i compiti ai singoli dipendenti affidati... ».

****

Di seguito i **LINK** ad alcune delle numerose sentenze e provvedimenti in tema di posta elettronica, vari commenti di autorevoli giuristi, sentenze emesse da corti Europee, al fine di dare un'idea dell'interesse e dell'orientamento della giurisprudenza in merito, e quanto questa influisce sugli aspetti tecnici delle e-mail e vice versa.

Questo capitolo verrà continuamente aggiornato on-line per i lettori di "Dynamic e-book", anche con il gradito contributo degli utenti, i quali verranno citati nell'apposita sezione ed in calce al contributo.

Come si vedrà la materia è ancora abbastanza sconosciuta ai giudici, visto l'elevato numero di sentenze contrastanti fra loro:

1) TRIBUNALE DI BRESCIA 11/03/2008 N. 348/08 *Il messaggio di posta elettronica "semplice", non certificato ai sensi del* D.P.R. *Il*

febbraio 2005, n. 68, e privo di firma digitale a crittografia asimmetrica ai sensi del D.Lg. 7 marzo 2005, n. 82, non può fornire alcuna certezza circa la propria provenienza o sull'identità dell'apparente sottoscrittore, e pertanto non può essere qualificato alla stregua di atto pubblico.
http://www.penale.it/page.asp?mode=1&IDPag=604

2) CORTE DI CASSAZIONE SEZIONE LAVORO 19/02/2008, n. 4061 "*E' valida la comunicazione di cancelleria ex art. 136 c.p.c., effettuata per e-mail all'indirizzo elettronico comunicato dal difensore al proprio Consiglio dell'Ordine e da questi alla Corte d'Appello competente, a norma del D.P.R. 13 febbraio 2001, n. 123, artt. 2, 4, 6, del quale il destinatario ha dato risposta per ricevuta non in automatico, documentata dalla relativa stampa cartacea*".
http://www.altalex.com/index.php?idnot=41431

3) CORTE DI CASSAZIONE SEZ. LAVORO N. 1145/01 *Quale valore probatorio ha il messaggio di posta elettronica ai fini del licenziamento? Commento alla sentenza della cassazione n. 1145/01*
http://www.lavoroprevidenza.com/leggi_articolo.asp?id=328

4) TRIBUNALE DI CATANIA, SEZIONE LAVORO, 2 FEBBRAIO 2009 *"Il dipendente RSU può inviare, utilizzando il suo indirizzo personale di posta elettronica, comunicazioni sindacali a mezzo di e-mail ai dipendenti della società durante il loro orario di lavoro e al loro indirizzo aziendale di posta elettronica"*
http://www.coisp.it/sentenze/Divulgazione%20tramite%20e-mail%20attivit%C3%A0%20sindacale%20durante%20orario%20di%20lavoro%20-%20Sent.%202%20feb%2009..pdf

5) CORTE DI CASSAZIONE, SEZIONE QUINTA PENALE, n. 46674 del 14/12/ 2007 *Un anno di reclusione per chi crea un account di posta elettronica con falsa identità. Ingannare altri utenti di internet costituisce il reato di sostituzione di persona*
http://www.guardieinformate.net/modules/newbb/viewtopic.php?viewmode=flat&topic_id=2197&forum=22

6) CASS. SEZ. LAVORO N. 4375 DEL 23 FEBBRAIO 2010 *Licenziamento disciplinare a seguito di contestazione per uso di internet durante l'orario di lavoro non collegato ad esigenze aziendali. Rilevazione*

dell'illecito attraverso un programma di controllo centralizzato. Violazione dell'art. 4 dello statuto dei lavoratori. Sussiste. inutilizzabilità dei dati acquisiti con il programma di controllo. sanzione eccessiva anche in relazione alla durata dei collegamenti ed ai precedenti disciplinari del lavoratore. sussiste.
http://www.ordinecdlna.it/sentenze00/n%202%20DEL%202010.pdf

7) La sentenza dell'High Court of Justice in "Mehta v. J Pereira Fernandes S.A. "emessa il 7 aprile 2006", enuncia i motivi logici per la constatazione istintiva che l'indirizzo del mittente su un E-mail non può costituire firma della stessa. Questa sentenza mostra anche l'operatività e flessibilità della Common Law, in un contesto molto moderno.
http://www.filodiritto.com/index.php?azione=visualizza&iddoc=301

8) CORTE DI CASSAZIONE SEZIONE PENALE N. 1369/2009 *Siffatto principio giuridico, ivi enunciato in riferimento al diritto di cronaca spettante al giornalista, per la sua ampia portata si rende applicabile anche in ogni caso in cui si prospetti il legittimo esercizio del diritto di critica: il che non si traduce nel privare di operatività in via generale la regola di cui al primo comma dell'art. 596 c.p., o le eccezioni a detta regola contenute, operando l'una e le altre quando non siano invocabili il diritto di cronaca o di critica (cass. 12 dicembre 1986, A.).*
http://www.alphaice.com/giurisprudenza/?id=7638

9) TRIBUNALE DI TORINO N. 143/2006 15 .09 2006 *L'e-mail aziendale appartiene al datore di lavoro. In relazione al reato di cui all'art. 616 c.p. il fatto non sussiste qualora, anche in presenza di adeguata policy aziendale, il datore di lavoro acceda alla casella personalizzata del dipendente.*

10) CASSAZIONE 22/02/2010 N° *4375 I programmi informatici che consentono il monitoraggio della posta elettronica sono soggetti all' art.4 dello statuto dei lavoratori*
http://bernericonsulting.com/general/cassazione-e-controllo-dei-lavoratori-615

11) La giurisprudenza europea sull'art. 5.2 della direttiva 93/99 http://www.interlex.it/docdigit/r_manno12.htm

12) CASSAZIONE SEZIONE V PENALE 14/12/ 2007, n. 46674 Sostituzione di persona attraverso posta elettronica http://www.altalex.com/index.php?idnot=39435

EPILOGO
LA FINE DELLA POSTA ELETTRONICA

COSA SOSTITUIRÀ LA POSTA ELETTRONICA?

L'E-mail ha fatto il suo tempo come incontrastata "Regina della comunicazione" dopo oltre 10 anni di effettivo servizio, era stata inventata molti anni prima, ma il suo regno è veramente finito?
Al suo posto, una nuova generazione di servizi sta iniziando a prendere piede, servizi come Twitter e Facebook e molti altri in lizza fra loro per aggiudicarsi un pezzo importante del nuovo mondo delle comunicazioni; persino Gmail, sinonimo dell'e-mail libera e sicura, si trasforma in Voip e chat on-line. Proprio come la posta elettronica ha fatto più di un decennio fa, questo spostamento promette di riscrivere profondamente il nostro modo di comunicare, in modi, in cui possiamo solo immaginare la portata e gli effetti.
Perseverare in un errore è diabolico, voler per forza creare delle leggi che regolano la tecnologia è da idioti. Richiamando ancora una volta quanto detto dall'amico Franco Bassanini ed aggiungendo qualcosa di mio: "Le Leggi non viaggiano alla stessa velocità della tecnologia, non la possono né imbrigliare, né fermare, sarebbe un'idiozia". Su questa massima coniata da *Franco Bassanini* e da me rivista, c'è da pensare e riflettere, il perché ed il significato di questo.

Iniziamo da un esempio classico e fruibile da tutti, che riguarda proprio la più semplice e rivoluzionaria invenzione dei sistemi di comunicazione: il telefono.

Ricordate come era il telefono, senza ritornare ai tempi di Meucci, ma anche per cercare come lui, di non farci bruciare l'invenzione, quella che doveva essere la rivoluzione digitale i primi del 1997? Siamo molto bravi in questo! Che cosa è avvenuto in CINA? Il Paese, che all'epoca, era l'ultimo in questo campo come linee e telefoni installati.

La vera INNOVAZIONE!

1) *Reti telefoniche in fibra ottica*
2) *Centrali di nuovissima concezione*
3) *Banda larga ed accesso ad Internet*
4) *Ma soprattutto il Telefono digitale sia pubblico che privato*

In sintesi, l'applicazione delle ultime tecnologie esistenti. A nessuno in CINA gli è venuto in mente di iniziare con una rete in rame e di installare telefoni (come quello che si vede nella figura) o cabine telefoniche con telefoni a gettoni.

Dando per assunto che la Posta Elettronica è stata inventata nel 1972 e quindi, in epoca molto remota rispetto alla sviluppo di Internet, ***questo è invece quanto è accaduto e accade oggi in Italia:***

- ***Nel 1997 Franco Bassanini, per primo in Europa, fece promulgare la legge su quella che doveva essere la Rivoluzione Digitale nel nostro paese. Dieci anni dopo, nella conferenza "1997-2007 – DIECI ANNI DI DOCUMENTI INFORMATICI A CHE PUNTO SIAMO CON L'AMMINISTRAZIONE DIGITALE?" le sue dichiarazioni nel video***:

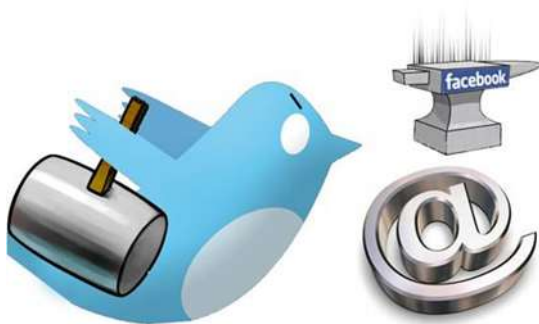
http://www.cittadininternet.it/?p=260

- ***Nel 2005 abbiamo inventato la PEC Posta Elettronica Certificata***
- ***Nel 2009 qualcuno se ne è "innamorato" e la vuole distribuire a tutti gli Italiani, anzi lo sta facendo, come il massimo del progresso tecnologico, che avanza indifferente alle nostre lungaggini burocratico legislative.***
- ***Tra breve e già oggi, la Posta Elettronica è ufficialmente dichiarata obsoleta e destinata ad essere soppiantata da altre tecnologie.***

TUTTO QUESTO SI CHIAMA INNOVAZIONE?

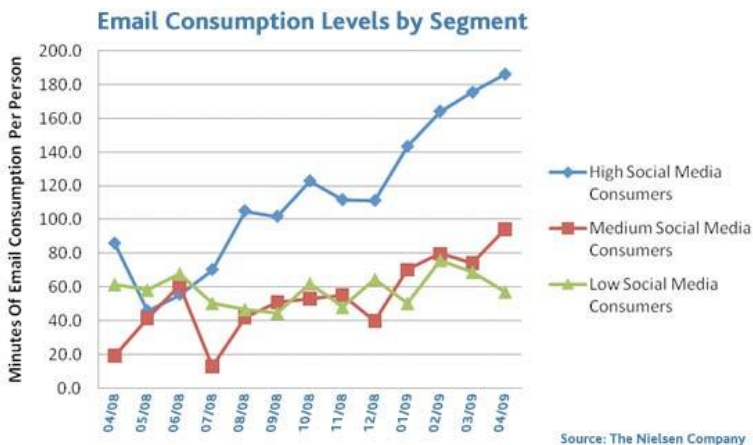
IL RUOLO DEI SOCIAL NETWORK NELLA COMUNICAZIONE GLOBALE

Vediamo cosa succede con l'inarrestabile corsa della tecnologia che non aspetta sicuramente l'evolversi delle nostre leggi, regolamenti, norme di ogni genere.

Un'importante asserzione del COO di Facebook Sheryl Sandberg (vedi immagine e video: http://www.cittadininternet.it/?p=724) conferma quanto era già nell'aria: la fine della Posta Elettronica, almeno così come è concepita ed usata oggi. Forse l'asserzione di Sheryl può apparire interessata, stante la sua posizione, ma questo viene ampliamente supportato da altre fonti autorevoli. Iil Wall Street Journal confermava, già da tempo, questa logica tendenza, sostenendo che Facebook e Twitter, che ora sono gli incontrastati leader della comunicazione online ("l'e-mail ha avuto la sua vita … ma il suo regno è finito"), fa eco Sandberg, non sono i primi a fare questa affermazione. Basta fare una ricerca rapida su Google, e si troveranno una miriade di informazioni, blog ed altro ancora, in tutte le lingue, oltre ad una marea di giochi di parole che annunciano che dovremmo usare sistemi diversi per sopravvivere, dare addio alle e-mail ed altro ancora.

L'E-mail è davvero finita?

Secondo Sandberg, solo l'11% dei giovani invia e-mail ogni giorno, serie ed inoppugnabili statistiche vedono senza ombra di dubbio il passaggio agli SMS, ormai gestiti attraverso sistemi di Comunicazione Unificata, anche sul PC Aziendale e tutti i social network.

Nel 2005, un ***altro serio studio di Forbes*** [107] *confermava, che meno del 5% degli adolescenti americani tra i 12-17 preferivano l'Instant Messaging per la comunicazione digitale, rispetto alle e-mail.*
Ora, cinque anni dopo, molti di questi giovani stanno entrando nel mondo degli affari e del lavoro, ma non abbiamo visto AIM, Yahoo Messenger, e G-Chat, Facebook ecc. superare l'e-mail, almeno non ancora.
Uno studio della Nielsen Co. sulle e-mail in Australia, Brasile, in diversi paesi europei, e negli Stati Uniti, ha rilevato che l'utilizzo delle stesse è aumentato del 21% tra agosto 2008 ad agosto 2009, raggiungendo 276,9 milioni di utenze.
Nello stesso periodo, la percentuale degli utenti dei siti di social-network è balzato a 301,5 milioni di persone. A causa di questa forte crescita, le comunità di Internet come Facebook, riescono ad abbassare la quantità di tempo che gli utenti trascorrono nella comunicazione attraverso i tradizionali servizi di messaggistica come le E-mail. I dati parlano chiaro se si considera che tra il 2003 e il 2009, il tempo speso per gestire le e-mail è ***sceso del 41%****, di contro i "social network occupano un tempo pari a* ***l 22% del totale degli utenti Internet di tempo****, contro al 24% rispetto all'anno scorso.*

Ecco le statistiche:

In un altro recente studio, Nielsen, tuttavia, ha determinato (vedi grafico,) che in un certo qual modo, i social network hanno contribuito ad aumentare l'uso della posta elettronica in senso assoluto. In una prima analisi sembrava che aumen-

107 http://www.forbes.com/2005/07/29/teens-email-habits-cx_ld_0729digilife.html

tando il numero di utenti nei social network facesse diminuire l'uso della posta elettronica, i risultati come si vede sono diversi da quello che ci si aspettava.
"Abbiamo deciso di sfornare alcuni dati resoconto" di testare la nostra ipotesi che "il consumo dei social media si riduce all'uso della posta elettronica", ha spiegato Jon Lardoni, VP analisi dei dati multimediali di Nielsen. "Sembra in effetti che i social network facciano aumentare gli account e-mail e l'uso delle stesse. "
A complicare ulteriormente la situazione, alcune società di ricerche di mercato, come il famoso Radicati Group che **ha diffuso un rapporto nel mese di aprile** *stimando che le reti sociali cresceranno ad un ritmo notevole nei prossimi anni – ma ha anche mostrato che l'utenza della posta elettronica, in tutto il mondo, aumenterà in modo notevole:"Il numero degli account di posta elettronica a livello mondiale dovrebbe aumentare di oltre 2,9 miliardi nel 2010, a oltre 3,8 miliardi entro il 2014".*
"Tuttavia, il Social Networking rappresenta attualmente la più veloce tecnologia di comunicazione tra i consumatori e gli utenti business, con oltre 2,1 miliardi si stima nel 2010, si prevede un'ulteriore crescita a oltre 3,6 miliardi entro il 2014."

Pur aumentando in senso assoluto, la relazione del gruppo Radicati ha anche mostrato come l'uso quotidiano delle e-mail è diminuita, sia per il mercato consumer, che business - evidente l'influenza della messaggistica attraverso i social network.

TEMPI DI CONNESSIONE CON I PIU POPOLARI BRAND ON-LINE AD APRILE 2010		
Brand	Visita degli utenti per Brand	Tempi per utente per brand
Google	82%	1:21:51
MSN/ WindowsLive/Bing	62%	2:41:49
Facebook	54%	6:00:00
Yahoo!	53%	1:50:16
Microsoft	48%	0:45:31
YouTube	47%	0:57:33
Wikipedia	35%	0:13:26
AOL Media Network	27%	2:01:02
eBay	26%	1:34:08
Apple	26%	1:00:28
Fonte: The Nielsen Company *Paesi oggetto dell'indagine AU, BR, CH, DE, ES, FR, IT, UK & USA only		

Su tutto questo c'è da fare un'importante considerazione di carattere tecnico, che ai miei eminenti colleghi è evidentemente sfuggita.

Come funziona il sistema: Chi si connette ad un social Network, es. Facebook, possiede per forza un' e-mail normale, sia essa una web mail gratuita tipo G-mail, che una di tipo aziendale, chi non c'è l'ha è obbligato ad averne una. Inoltre, molto spesso proprio per i social network viene presa un'e-mail ad hoc per tutta una serie di plausibili motivi.
Tutta questa snocciolata di cifre, che i miei colleghi di oltre oceano piace tanto, non tiene conto di questo semplice fatto, in cui: aumentando il numero dei Social Networker, aumentano anche il numero degli utenti e-mail, inclusi quelli che magari non pensavano di farsene una.
Nessuno è riuscito a scindere questi dati, cioè il vero aumento di coloro che NON avrebbero mai pensato di avere un'e-mail, ma per usare ad esempio FB debbono averne per forza una.
Sull'aumento del numero delle e-mail che girano in rete si sono dimenticati di un altro paradosso, chi ha un indirizzo e-mail ed accede a Facebook, può chiedere al sistema che ogni messaggio transiti su Facebook, gli arrivi una notifica ANCHE PER E-MAIL ad ogni iterazione prevista dal sistema, da qui la probabile stima, quasi impossibile da rilevare, dei due dati, uno che scende l'altro che aumenta od il contrario. Mancano infatti, i riferimenti precisi su

quanti hanno scelto queste opzioni, che fanno gioco forza, crescere e "drogare" le stime:

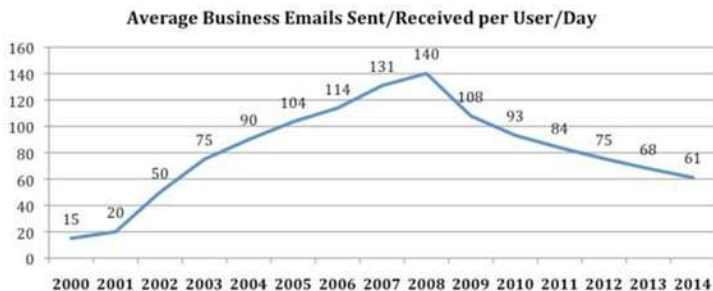
- *Del numero degli account di e-mail esistenti nel mondo*
- *I tempi in cui l'utente dedica alla gestione delle e-mail, se si pensa che ogni messaggio in transito su FB produce un messaggio e-mail (es. ogni nuovo amico, invito ad eventi, la formazione di un nuovo gruppo ed altro ancora).*

Se si aggiunge che la messaggistica SMS molto spesso viene gestita tramite sistemi di comunicazione unificata, anche questi vanno a ledere i dati, per non parlare dei fax ormai anche questi inseriti in sistemi e-mail.
In questo modo con la moltiplicazione della messaggistica è difficile stabilire cosa stia veramente avvenendo.

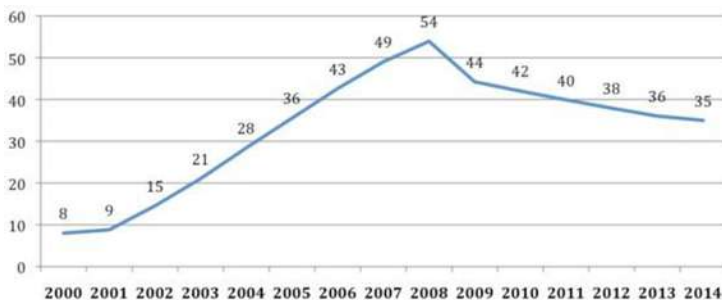
I grafici che seguono non sono influenzati da questa mia opinione ed a mio avviso non rappresentano la realtà, cioè la progressiva scomparsa del sistema e-mail tradizionale. Un altro aspetto interessante, che ci riguarda da vicino, è l'uso dei Social Network, in cui siamo al secondo posto al mondo, diveniamo i primi sostenitori di Facebook in assoluto, conseguentemente i primi ad usare sistemi alternativi alle e-mail tradizionali:

Reach and Usage by Country / Apr 2010 (Home & Work)
Social Networking / Blog Sites

Country	% Reach of Active Users	Time per Person (hh:mm:ss)
Brazil	86%	5:03:37
Italy	78%	6:28:41
Spain	77%	5:11:44
Japan	75%	2:50:50
United States	74%	6:35:02
United Kingdom	74%	5:52:38
France	73%	4:10:27
Australia	72%	7:19:13
Germany	63%	4:13:05
Switzerland	59%	3:43:58

Source: The Nielsen Company

Media del numero di e-mail (business) inviate / ricevute per utente / giorno

Nel futuro, malgrado le diverse opinioni, mi pare sia inarrestabile la corsa verso un sistema unificato di comunicazione, che abbia come effetto immediato la fine dell'e-mail, così come attualmente ideata e gestita. Saranno i social Network a sostituire l'e-mail tradizionale (questa è già una realtà), un interessante ***contributo da Zack Whittaker*** *dal titolo significativo, che lascio in originale,"Generation Y: 'E-mail is unfashionable and outdated'.*

Annunci si susseguono ogni giorno, gmail diviene Voip, ma anche chat on-line ed altri ancora.
Dopo tutto, cosa è "l'e-mail"? Oggi, servizi come Gmail includono elementi di chat, aggiornamenti status, editing, funzionalità diverse ed altro ancora, per non parlare poi del recente annuncio di Gmail che diventa VOIP, ma anche messaggistica e poi ***googlewav****e. Ll'avete provato? - è impossibile definire chiaramente cosa rende una rete sociale, e cosa rende un servizio e-mail.*

Media del numero di e-mail (consumer) inviate/ricevute per utente/giorno

Facebook Reach and Usage by Country / Apr 2010 (Home & Work)

Country	% Reach of Active Users	Time per Person (hh:mm:ss)
Italy	66%	7:00:21
Australia	63%	7:45:28
United States	62%	6:43:22
United Kingdom	62%	6:19:59
Spain	57%	4:04:53
France	57%	4:33:05
Switzerland	45%	4:18:47
Germany	27%	3:42:50
Brazil	26%	1:46:50
Japan	3%	0:31:38

Source: The Nielsen Company

Arrivati a questo punto molti mi hanno chiesto e molti mi chiederanno: "…, ma in un momento come questo in cui asserisci che l'e-mail è morta, ti metti a scrivere proprio un libro intitolato La Posta Elettronica?" La risposta istintiva a questo interrogativo è: "Un libro ha più successo quando si parla di qualcosa che è morto soprattutto di recente."
A parte questa scontata battuta, forse anche un po' macabra, direi che il mio libro oltre a voler essere una sorta di "epitaffio" della posta elettronica, così come oggi concepita, è anche la conferma della teoria che la tecnologia avanza in barba alle leggi di questo paese e conseguentemente, va usata l'ultima tecnologia disponibile.
Cosa impossibile se si creano norme che impediscono che questo avvenga. Forse il titolo poteva essere diverso, ma parliamo sempre dell'eterna ricerca umana della comunicazione, dell'incontro del non essere e rimanere soli in un mondo sempre più popolato e sempre più interconnesso, un contro senso od un utopia, forse la fine di un'era o l'inizio di un altra.
Non temete, il mio non è un libro di filosofia, ma quanto sta avvenendo mi fa e ci deve far pensare. Questo ed altro potrete leggere nel mio libro che sarà oltre che distribuito in forma cartacea, anche come e-book.

APPENDICI

Elenco dei più comuni POP3 E SMTP vedi pag. 62

SERVER	**POP3**	**SMTP**
GMAIL	pop.gmail.com	smtp.gmail.com (connessione ssl)
BLU	popmail.blu.it – pop.blu.it	mail.blu.it – smtp.blu.it
INWIND.IT	popmail.inwind.it	mail.inwind.it
LIBERO ADSL	popmail.libero.it – imapmail.iol.it -	mail.libero.it
LIBERO.IT	popmail.libero.it (POP solo se connessi a wind) – imapmail.iol.it	mail.libero.it
WIND.IT		
MSN HOTMAIL	pop3.live.com (port 995)	smtp.live.com (port 25)
MSN HOTMAIL IT		
TELECOM ADSL SMART	mail.cs.interbusiness.it	mail.tuttopmi.it
TELECOM BUSINESS	mail.191.it -	smtp.191.it o mail.191.it
TELECOM CASA		
TIM.IT	mail.posta.tim.it – box.posta.tim.it	box.posta.tim.it webmail1.posta.tim.it nel caso del servizio di posta UniTIM/iBox
ALICE ADSL	in.alice.it	out.alice.it
ROSSOALICE	in.aliceposta.it – box.tin.it	out.aliceposta.it mail.tin.it
TIN.IT	pop.tin.it – box.tin.it (alice-adsl) – box.clubnet.tin.it – box2.tin.it (Da pop si scarica gratis solo se ti connetti con tin.it)	smtp.tin.it (?) mail.tin.it (aliceadsl) mail.clubnet.tin.it
VIRGILIO	in.virgilio.it – popmail.virgilio.it	out.virgilio.it smtp.virgilio.it
TISCALI ADSL – FREE/FLAT	pop.tiscali.it	smtp.tiscali.it

SERVER	**POP3**	**SMTP**
TISCALI.IT	pop.tiscali.it	smtp.tiscali.it
TELE2 ADSL	pop.tele2.it	smtp.tele2.it
ALICE.IT	in.alice.it	
ALICEPOSTA.IT	in.alice.it	
JUMPY.IT	pop.jumpy.it	mail.jumpy.it
KATAWEB.IT	mail.katamail.com – pop.katamail.com	smtp.katamail.com
LYCOS	pop.lycos.it – pop3.lycos.it	smtp.lycos.it
MICROSOFT		
MSN.COM	smtp.e-mail.msn.com	pop3.e-mail.msn.com
SUPEREVA.IT	mail.supereva.it	mail.supereva.it
TELE2 EVER-YDAY	pop.tele2.it	smtp.tele2.it
VODAFONE MAIL	popmail.vodafone.it – (pop3.vizzavi.it old)	smtp.net.vodafone.it (smtpmail.vodafone.it smtp.vizzavi.it old)
VODAFONE.IT	popmail.vodafone.it	smtpmail.vodafone.it
YAHOO.COM	pop.mail.yahoo.com	smtp.mail.yahoo.com
YAHOO.COM.CN	pop.mail.yahoo.com.cn	
YAHOO.IT	pop.mail.yahoo.it	smtp.mail.yahoo.it Se ISP ha bloccato la porta 25 modificare porta SMTP del client ed utilizzare la 587
1UND1.DE	pop.1und1.de	
ABES.IT	mail.abes.it	
ACCESS4LESS		smtp.access4less.net
ACTIVE NETWORK		smtp.activenetwork.it
ADELPHIA		mail.adelphia.net
AERASRL.IT	mail.aerasrl.it	
AGENZIAZU-	pop.agenziazurich.it	

SERVER	**POP3**	**SMTP**
RICH.IT		
A-ICE.AERO	pop3.panservice.it	
ALBACOM		relay.albacom.net smtp.albacom.net
ALCOTEK.IT	pop3.alcotek.it	
ALLMEDIASOLU-TION.COM	pop.allmediasolution.com	
ALTEVIE.COM	mail.altevie.com	
AMNESTY.IT	library.amnesty.it	
ANONI-MAGDR.COM	pop3.anonimagdr.com	
ARPA.SICILIA.IT	arpa.sicilia.it	
ART-BIT.NET	mail.art-bit.net	
ARUBA.IT	pop3.aruba.it	smtp.aruba.it
ASP.IT	mail.asp.it	
ASSOGROUP.SM	mail.assogroup.sm	
ASTRANET.IT	mail.astranet.it	
ATLAVIA		smtp.atlavia.it
AUBAY.IT	pop.aubay.it	
AUNA		smtp.auna.com
AUTOMATASPA.IT	pop3.automataspa.it	
BANGLA-DESH.NET	mail.bangladesh.net	
BCCSANTERA-MO.IT	pop.bccsanteramo.it	
BELLSOUTH		mail.bellsouth.net
BERNARDISRL.IT	mbox.edbusiness.it	
BERTAIOLA.COM	pop3.bertaiola.com	
BFSINFORMATI-CA.COM	pop3.bfsinformatica.com	
BLIXER.IT	mail.blixer.it	
BLUEBOTTLE		mail.bluebottle.com
BLUELIGHT.COM		smtp.mybluelight.com

SERVER	**POP3**	**SMTP**
BMSITALIA.COM	www.bmsitalia.com	
BOL.COM.BR		smtp.bol.com.br
BONBON.NET	pop.bonbon.net	
BSC.IT	mail.bsc.it	
BTTB		mail.bttb.net.bd
CAIWAY		smtp.caiway.nl
CALTANET.IT	mbox.caltanet.it	relay.caltanet.it
CANTV.NET		mail.cantv.net
CHARTER	pop.charter.net	mail.charter.net
CHEAPNET.IT	pop.cheapnet.it	smtp.cheapnet.it
CHIPSOLU-TION.IT	chipsolution.it	
CIAOWEB	ciaopop3.ciaoweb.it – pop3.ciaoweb.net	ciaosmtp.ciaoweb.it smtp.ciaoweb.net mail.ciaoweb.net
CITIESONLINE.IT		
CIUDAD		smtp.ciudad.com.ar
CLEFFE.IT	pop3.cleffe.it	
CLUB-INTERNET		smtp.club-Internet.fr
COAS.IT	mail.coas.it	
COCCO.IT	cocco.it	
COLDIRETTI.IT	pop3.coldiretti.it	
COLUMBIA POWER AND WA-TER		mail.cpws.net
COMCAST		smtp.comcast.net
COMELLIASSICU-RAZIONI.IT	pop3.comelliassicurazioni.it	
COMM2000.IT	pop.comm2000.it	
CORRE-O.YAHOO.ES	pop.correo.yahoo.es	
CSINFORMAZIO-NI.IT	popmail.csinformazioni.it	
CUORINAVIGAN-	pop3.cuorinaviganti.it	

SERVER	**POP3**	**SMTP**
TI.IT		
DDS.NL	pop3.dds.nl	
DEEJAYMAIL.IT	pop.deejaymail.it	
DEEPTUNING.IT	pop3.deeptuning.it	
DIEBSPIEL24.DE		
DIMI.UNIUD.IT	ten.dimi.uniud.it	
DISP.UNIROMA2.IT	mail.disp.uniroma2.it	
DRINKPINKONLINE.COM	pop3.drinkpinkonline.com	
EARTSTUDIO.IT	pop3.eartstudio.it	
EASYNET.RO	pop.easynet.ro	
ECOM.IT	pop.ecom.it	
ECORETE.IT	pop.ecorete.it	
EDIMEDIA.COM	mail.edimedia.com	
EKAR.IT	mail.ekar.it	
ELITEL	pop.elitel.it	smtp.elitel.it smtp.elitel.biz
E-MAIL.IT	popmail.e-mail.it	smtp.e-mail.it
ETNOTEAM.IT	pop.inet.it	
EUSTEMA.IT	pop.eustema.it	
EXCITE	pop.tiscali.it	smtp.tiscali.it
FASTMAIL		mail.messagingengine.com
FASTWEB	pop.fastwebnet.it	smtp.fastwebnet.it
FIBERTEL.COM.AR		smtp.fibertel.com.ar
FIN-INNOVATIONS.COM	pop.fin-innovations.com	
FINSA.IT	mail.finsa.it	
FIRENZE.NET	pop3.izymail.com	
FLAXMODEL.COM	mail.flaxmodel.com	

SERVER	POP3	SMTP
FREE		smtp.free.fr
FREE-MAIL.IT	free-mail.it	
FREENET.DE		mx.freenet.de
FREEPASS.IT	pop3.freepass.it	
FUORISSIMO.COM		
GABAMA.COM	ilmarsupio.gabama.com	
GALACTICA.IT	mail.galactica.it	mail.galactica.it
GAZETA.PL	pop3.poczta.gazeta.pl	
GIGA		smtp.giga.net.tw
GMX.DE	pop.gmx.net	
GMX.IT	pop.gmx.it	mail.gmx.it
GMX.NET	pop.gmx.net	mail.gmx.net
GO.COM		smtp.go.com
GRUPPOA-CSI.COM	www.gruppoacsi.com	
GRUPPOSISTE-MATICA.IT	mail.grupposistematica.it	
GUIDODELLA-VOLPE.COM	pop3.guidodellavolpe.com	
HAIER ELEC-TRONICS		smtp.haier-electronics.com
HINET		ms1.hinet.net – msa.hinet.net
HOME.RO	mail.home.ro	
HOTPOP.COM	pop.hotpop.com	smtp.hotpop.com
IAMONLINE.IT		
ICQMAIL.COM		
IG		smtp.ig.com.br
IINI.COM	mail.iini.com	
ILGIORNALEDI-CINISI.IT	pop3.ilgiornaledicinisi.it	
INFINITO.IT	pop3.infinito	smtp.infinito
INFOMEDIA.IT	handsoff.infomedia.it	

SERVER	**POP3**	**SMTP**
INTERBUSINESS TI EASYNET (TIN)	mail1.cs.interbusiness.it	
INTERFREE.IT	mail.interfree.it	mail.interfree.it
INTERNETLIBE-RO	mail.Internetlibero.it	smtp.Internetlibero.it
INTRAGE.COM	pop.intrage.com	
IOL	popmail.iol.it	mail.iol.it
ISAFSRL.COM	pop3.isafsrl.com	
ISTCONSUL-TING.IT	pop.istconsulting.it	
ISTRUZIONE.IT	pop.istruzione.it	
ITALYMAIL		mail.italymail.biz
ITSTAFF.IT	pop.itstaff.it	
IXPRES.COM		smtp.ixpres.com
JUNO.COM		
KAINESHA-DOW.IT	pop3.kaineshadow.it	
KATAMAIL.COM	pop.katamail.com	
KLIK	mail.klik.it	smtp.klik.it
LIBERTYSURF.FR	pop.libertysurf.fr	
LIFEGATE.IT	mail.lifegate.it	
LILLINET		smtp.weblinea.it
LOKISRL.COM	pop3.lokisrl.com	
LOMBARDIACOM	smtp.lombardiacom.it	pop.lombardiacom.it
LUCULLO.IT	mail.lucullo.it	
MACISTE	mail.maciste.it	
MACROMEDIA		
MAIL.COM		
MAIL.RU	pop.mail.ru	
MAILSNARE		mail.mailsnare.net
MAN-CON.COM	pop3.man-con.com	
MC3INFO.COM	pop.mc3info.com	
MCLINK	mail.mclink.it	mail.mclink.it
METACRAWLER		

SERVER	**POP3**	**SMTP**
METEONE-TWORK.IT	mail.meteonetwork.it	
METSYSTEM.IT	mail.metsystem.it	
MOMAX		smtp.momax.it
MONRIF.NET	mail.monrif.net	mail.monrif.net
MONTELIBRET-TI.ORG	mail.montelibretti.org	
MONZA.NET	pop.metropolink.com	
MSOFT.IT		smtp.weblinea.it
MULTITECH.IT	mail.multitech.it	
MULTITECH-AD.COM	mail.multitech-ad.com	
MUNDOFRE-E.COM	pop3.mundofree.com	
NAFURA.IT	pop.nafura.it	
NEOMEDIA ADSL	neomedia.it	neomedia.it
NET2B.PT	net2b.pt	
NET4FREE	smtp.net4free.it	pop.net4free.it
NETCOMSOLU-TION.IT	mail.netcomsolution.it	
NETEK.IT	pop.netek.it	
NETEXPLORA CHILE		mail.netexplora.com
NETVIGATOR		mail.netvigator.com
NETVIS+O (POR-TUGAL)		mail.netvisao.pt
NETZERO.COM		smtp.netzero.com
NEWS.INDIVIDUAL.NET		
NEXT.DOM	mail.next.it	
NEXT.IT	mail.next.it	
NGI.IT	popnew.ngi.it	smtp.ngi.it
NOPAY	mail.nopay.it	mail.nopay.it
NTL (UK)		smtp.ntlworld.com

SERVER	**POP3**	**SMTP**
OKSATCOM.IT	pop.oksatcom.it	
ONE-ANS.IT	mailserver.one-ans.it	
ONO		smtp.ono.com
OPERA21.IT	mail.opera21.it	
OPERAMAIL		
ORANGE-TECH.COM	pop3.orange-tech.com	
OU-TGOING.VERIZON.NET		tchrshelli
PELLIGRARO-BERTO.IT	webmail.pmiweb.it	
PEOPLE-VENE	mail.people.it	TuoProvider
POCHTAMT.RU	pop3.pochta.ru	
POCZTA.ONET.PL	pop3.poczta.onet.pl	
POST MAN		mail.postman.net
POSTE.IT	relay.poste.it	relay.poste.it
POSTINO.IT	pop.postino.it	smtp.postino.it
PREITO.COM	mail2.preito.com	
PROGETTOCASA-SNC.COM	mail.progettocasa-snc.com	
PROTOCOL.IT	mail.protocol.it	smtp.protocol.it
QUIPO.IT	quipo.it	quipo.it
R (CABLE GALI-CIA)		smtp.mundo-r.com
RADIO DEEJAY MAIL		smtp.deejaymail.it
RAGIONIERI.COM	posta.ragionieri.com	
RCP (PERU)		amauta.rcp.net.pe
REPLY.IT	owas.reply.it	
RETEITALY		smtp.reteitaly.com
REZIA.IT	mail.rezia.it	
RIBESINFORMA-TICA.IT	mail.ribesinformatica.it	

SERVER	**POP3**	**SMTP**
RIMINI.COM	mail.rimini.com	smtp.rimini.com
ROCKET-MAIL.COM	POP E l'SMTP non esisto-no	
RUNBOX		smtp.runbox.com
SAILOR	smtp.freepass.it	pop3.freepass.it
SALESIANI.IT	pop.salesiani.it	
SBC YAHOO DSL		smtp.sbcglobal.yahoo.com
SEDIIN.IT	mail.sediin.it	
SERCO.IT	mail1.serco.it	
SHYLEX TELE-COMUNICACIO-NES		smtp.shylex.net
SICILYONLINE.IT	pop3.sicilyonline.it	
SIFREE.IT		smtp.simail.it
SIFY.COM		mail.satyam.net.in
SIMAIL.IT	pop3.simail.it	
SIMAXSRL.COM	simaxsrl.com	
SIMOPALA.IT	pop3.simopala.it	
SIOR.IT	mail.sior.it	
SKYNET.BE		relay.skynet.be
SOFTHOME.NET	pop.SoftHome.net	smtp.SoftHome.net mail.softhome.net
SOUTHWESTERN BELL		mail.swbell.net
SPACEINFORMA-TICA.COM	pop3.spaceinformatica.com	
SPYMAC.COM	mail.spymac.com	mail.spymac.com
SQUALEX.COM	pop3.squalex.com	
STINGER-GROUP.NET	pop3.stingergroup.net	
STINGER-IT.COM	pop3.stinger-it.com	
STUDIOLURA-GHI.IT	pop3.studioluraghi.it	

SERVER	**POP3**	**SMTP**
SUNRISE (CH)		smtp.sunrise.ch
SYMPATICO		smtp1.sympatico.ca
TARIFFENET.IT	mail.tariffenet.it	
TDC		backup-mx.post.tele.dk
TECHEDGE.IT	mail.techedge.it	
TECREDO.COM	pop3.tecredo.com	
TELEFONICA		smtp.telefonica.net
TELE-NET(BELGIUM)		uit.telenet.be
TELEWEST		smtp.blueyonder.co.uk
TELKOM		smpt.telkom.net
TELUS		smtp.telus.net – mail.telus.net
TELVIA.IT		smtp.telvia.it
TEMPLA-RIOS.COM	mail.templarios.com	
TERRA – BR – RE-CIFE		smtp.rec.terra.com.br – smtp.sao.terra.com.br
TERRA – ESPAĐA		smtp.mailhost.terra.es
TERRA.COM		imap – smtp
TERRA.ES	pop3.terra.es	
TIMENET ADSL		smtp2.xdslnet.it
T-ONLINE		mailto.t-online.de
TOPCONSUL-TING.IT	mail.topconsulting.it	
TOUGHGUY.NET	pop.toughguy.net	
TRIM.IT	mailbus.fastweb.it	
TXT.IT	smtp.txt.it	
UNIROMA2.IT	pop.uniroma2.it	
USA.NET	pop.amexmail.com (a pa-gamento) SOLO WE-BMAIL	n/a
UTU.FI		smtp.utu.fi

SERVER	**POP3**	**SMTP**
VEBE	mail.people.it	
VERIZON DSL		outgoing.verizon.net
VI.NET	mail.vi.net	
VIC-NORA.IT	pop3.vic-nora.it	
VIDEOBANK		videobank.it
VIOL.UZ	mail.viol.uz	
VIVACITY		pop.Vivacity.it
WANADOO (FRANCE)		smtp.wanadoo.fr
WAPPI.COM	mail.wappi.com	
WDBSYSTEM.IT	mail.wdbsystem.it	
WEB.DE		smtp.web.de
WEB-GRATIS.NET	mail.web-gratis.net	
WEBMAIL.INET.IT	pop.inet.it	smtp.inet.it
WEBMAIL.TRE.IT		smtp.tre.it
WEBZONE	michetti.webzone.it	151.99.135.2
WISYPROD.COM	pop3.wisyprod.com	
WOOOW.IT	pop.wooow.it	smtp.wooow.it
WORLDONLI-NE.IT	pop.worldonline.it	smtp.worldonline.it
WP.PL	pop3.wp.pl	
XMSG		
X-PRIVAT		mail.x-privat.org
XS4ALL		smtp.xs4all.nl mail.xs4all.nl
YA.COM		smtp.ya.com
ZERO.AD.JP		zero.ad.jp
ZONNET		smtp.zonnet.nl
ZZN.COM		

CODICE DELL'AMMINISTRAZIONE DIGITALE
DECRETO LEGISLATIVO 7 MARZO 2005, N. 82

TESTO VIGENTE

(redatto al solo fine di facilitare la lettura del Codice dell'amministrazione digitale a seguito delle modifiche ed integrazioni introdotte dal decreto legislativo 30 dicembre 2010, n. 235, pubblicato nel Supplemento ordinario n. 8 alla Gazzetta Ufficiale n. 6 del 10 gennaio 2010 ed indicate in carattere grassetto corsivo)

INDICE

Sezione III - Organizzazione delle pubbliche amministrazioni rapporti fra Stato, regioni e autonomie locali

12. Norme generali per l'uso delle tecnologie dell'informazione e delle comunicazioni nell'azione amministrativa.
13. Formazione informatica dei dipendenti pubblici.
14. Rapporti tra Stato, regioni e autonomie locali.
15. Digitalizzazione e riorganizzazione.
16. Competenze del Presidente del Consiglio dei Ministri in materia di innovazione e tecnologie.
17. Strutture per l'organizzazione, l'innovazione e le tecnologie.
18. Conferenza permanente per l'innovazione tecnologica.
19. Banca dati per la legislazione in materia di pubblico impiego.

Capo II - Documento informatico e firme elettroniche; ***trasferimenti***, libri e scritture

Sezione I - Documento informatico

20. Documento informatico.
21. Documento informatico sottoscritto con firma elettronica.
22. Copie informatiche di documenti analogici.
23. Copie analogiche di atti e documenti informatici.

23-bis. Duplicati e copie informatiche di documenti informatici.

23-ter. Documenti amministrativi informatici

23-quater. Riproduzioni informatiche

Sezione II - Firme elettroniche e certificatori

24. Firma digitale.
25. Firma autenticata.
26. Certificatori.
27. Certificatori qualificati.
28. Certificati qualificati.
29. Accreditamento.
30. Responsabilità del certificatore.
31. ***Vigilanza sull'attività dei certificatori e dei gestori di posta elettronica certificata.***
32. Obblighi del titolare e del certificatore.
33. Uso di pseudonimi.
34. Norme particolari per le pubbliche amministrazioni e per altri soggetti qualificati.

35. Dispositivi sicuri e procedure per la generazione della firma.
36. Revoca e sospensione dei certificati qualificati.
37. Cessazione dell'attività.

Sezione III – ***Trasferimenti di fondi***, libri e scritture
38. ***Trasferimenti di fondi***.
39. Libri e scritture.

Capo III - Formazione, gestione e conservazione dei documenti informatici
40. Formazione di documenti informatici.
40-*bis*. ***Protocollo informatico***
41. Procedimento e fascicolo informatico.
42. Dematerializzazione dei documenti delle pubbliche amministrazioni.
43. Riproduzione e conservazione dei documenti.
44. Requisiti per la conservazione dei documenti informatici.
44-bis. Conservatori accreditati

Capo IV - Trasmissione informatica dei documenti
45. Valore giuridico della trasmissione.
46. Dati particolari contenuti nei documenti trasmessi.
47. Trasmissione dei documenti attraverso la posta elettronica tra le pubbliche amministrazioni.
48. Posta elettronica certificata.
49. Segretezza della corrispondenza trasmessa per via telematica.

Capo V - Dati delle pubbliche amministrazioni e servizi in rete
Sezione I - Dati delle pubbliche amministrazioni
50. Disponibilità dei dati delle pubbliche amministrazioni.
50-bis. Continuità operativa.
51. Sicurezza dei dati.
52. Accesso telematico ai dati e documenti delle pubbliche amministrazioni.
53. Caratteristiche dei siti.
54. Contenuto dei siti delle pubbliche amministrazioni.
55. Consultazione delle iniziative normative del Governo.
56. Dati identificativi delle questioni pendenti dinanzi all'autorità giudiziaria di ogni ordine e grado.

57. Moduli e formulari.
57-bis. Indice degli indirizzi delle pubbliche amministrazioni.

Sezione II - Fruibilità dei dati
58. Modalità della fruibilità del dato.
59. Dati territoriali.
60. Base di dati di interesse nazionale.
61. Delocalizzazione dei registri informatici.
62. Indice nazionale delle anagrafi.

Sezione III - Servizi in rete
63. Organizzazione e finalità dei servizi in rete.
64. Modalità di accesso ai servizi erogati in rete dalle pubbliche amministrazioni.
65. Istanze e dichiarazioni presentate alle pubbliche amministrazioni per via telematica.

Sezione IV - Carte elettroniche
66. Carta d'identità elettronica e carta nazionale dei servizi.

Capo VI
Sviluppo, acquisizione e riuso di sistemi informatici nelle pubbliche amministrazioni
67. Modalità di sviluppo ed acquisizione.
68. Analisi comparativa delle soluzioni.
69. Riuso dei programmi informatici.
70. Banca dati dei programmi informatici riutilizzabili.

Capo VII - Regole tecniche
71. Regole tecniche.

Capo VIII - Sistema pubblico di connettività e rete internazionale della pubblica amministrazione
Sezione I - Definizioni relative al sistema pubblico di connettività
72. Definizioni relative al sistema pubblico di connettività.
73. Sistema pubblico di connettività (SPC).
74. Rete internazionale delle pubbliche amministrazioni.

Sezione II - Sistema pubblico di connettività SPC

75. Partecipazione al Sistema pubblico di connettività.
76. Scambio di documenti informatici nell'ambito del Sistema pubblico di connettività.
77. Finalità del Sistema pubblico di connettività.
78. Compiti delle pubbliche amministrazioni nel Sistema pubblico di connettività.
79. Commissione di coordinamento del Sistema pubblico di connettività.
80. Composizione della Commissione di coordinamento del sistema pubblico di connettività.
81. Ruolo del Centro nazionale per l'informatica nella pubblica amministrazione.
82. Fornitori del Sistema pubblico di connettività.
83. Contratti quadro.
84. Migrazione della Rete unitaria della pubblica amministrazione.

Sezione III - Rete internazionale della pubblica amministrazione e compiti del CNIPA

85. Collegamenti operanti per il tramite della Rete internazionale delle pubbliche amministrazioni.
86. Compiti e oneri del CNIPA.
87. Regolamenti.

Capo IX - Disposizioni transitorie finali e abrogazioni

88. Norme transitorie per la firma digitale.
89. Aggiornamenti.
90. Oneri finanziari.
91. Abrogazioni.
92. Entrata in vigore del codice.

IL PRESIDENTE DELLA REPUBBLICA

Visti gli articoli 76, 87 e 117, secondo comma, lettera r), della Costituzione;

Visto l'articolo 14 della legge 23 agosto 1988, n. 400, recante disciplina dell'attività di Governo e ordinamento della Presidenza del Consiglio dei Ministri;

Visto l'articolo 10 della legge 29 luglio 2003, n. 229, recante interventi in materia di qualità della regolazione, riassetto normativo e codificazione - legge di semplificazione 2001;

Vista la legge 7 agosto 1990, n. 241, recante nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi;

Visto il decreto legislativo 12 febbraio 1993, n. 39, recante norme in materia di sistemi informativi automatizzati delle amministrazioni pubbliche, a norma dell'articolo 2, comma 1, lettera mm), della legge 23 ottobre 1992, n. 421;

Visto il decreto legislativo 30 luglio 1999, n. 300, recante disciplina dell'attività di Governo e ordinamento della Presidenza del Consiglio dei Ministri;

Visto il testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa (Testo A), di cui al decreto del Presidente della Repubblica 28 dicembre 2000, n. 445;

Visto il decreto legislativo 30 marzo 2001, n. 165, recante norme generali sull'ordinamento del lavoro alle dipendenze delle amministrazioni pubbliche;

Visto il decreto legislativo 23 gennaio 2002, n. 10, recante attuazione della direttiva 1999/93/CE relativa ad un quadro comunitario per le firme elettroniche;

Visto il decreto legislativo 30 giugno 2003, n. 196, recante codice in materia di protezione dei dati personali;

Vista la legge 9 gennaio 2004, n. 4, recante disposizioni per favorire l'accesso dei soggetti disabili agli strumenti informatici;

Visto il decreto legislativo 20 febbraio 2004, n. 52, recante attuazione della direttiva 2001/115/CE che semplifica ed armonizza le modalità di fatturazione in materia di IVA;

Vista la preliminare deliberazione del Consiglio dei Ministri, adottata nella riunione dell'11 novembre 2004;

Esperita la procedura di notifica alla Commissione europea di cui alla direttiva 98/34/CE del 22 giugno 1998 del Parlamento europeo e del Consiglio, modificata dalla direttiva 98/48/CE del 20 luglio 1998 del Parlamento europeo e del Consiglio, attuata dalla legge 21 giugno 1986, n. 317, così come modificata dal decreto legislativo 23 novembre 2000, n. 427;

Acquisito il parere della Conferenza unificata, ai sensi dell'articolo 8, del decreto legislativo 28 agosto 1997, n. 281, espresso nella riunione del 13 gennaio 2005;

Sentito il Garante per la protezione dei dati personali;

Udito il parere del Consiglio di Stato, espresso dalla Sezione consultiva per gli atti normativi nell'adunanza del 7 febbraio 2005;

Acquisito il parere delle competenti Commissioni della Camera dei deputati e del Senato della Repubblica;

Vista la deliberazione del Consiglio dei Ministri, adottata nella riunione del 4 marzo 2005;

Sulla proposta del Ministro per l'innovazione e le tecnologie, di concerto con il Ministro per la funzione pubblica, con il Ministro dell'economia e delle finanze, con il Ministro dell'interno, con il Ministro

della giustizia, con il Ministro delle attività produttive e con il Ministro delle comunicazioni;

Emana il seguente decreto legislativo:

Capo I - Principi generali

Sezione I - Definizioni, finalità e àmbito di applicazione

1. *Definizioni.*

1. Ai fini del presente codice si intende per:

a) allineamento dei dati: il processo di coordinamento dei dati presenti in più archivi finalizzato alla verifica della corrispondenza delle informazioni in essi contenute;

b) autenticazione del documento informatico: la validazione del documento informatico attraverso l'associazione di dati informatici relativi all'autore o alle circostanze, anche temporali, della redazione;

c) carta d'identità elettronica: il documento d'identità munito ***di elementi per l'identificazione fisica*** del titolare rilasciato su supporto informatico dalle amministrazioni comunali con la prevalente finalità di dimostrare l'identità anagrafica del suo titolare;

d) carta nazionale dei servizi: il documento rilasciato su supporto informatico per consentire l'accesso per via telematica ai servizi erogati dalle pubbliche amministrazioni;

e) certificati elettronici: gli attestati elettronici che collegano all'identità del titolare i dati utilizzati per verificare le firme elettroniche;

f) certificato qualificato: il certificato elettronico conforme ai requisiti di cui all'*allegato I della* direttiva 1999/93/CE, rilasciati da certificatori che rispondono ai requisiti di cui all'allegato II della medesima direttiva;

g) certificatore: il soggetto che presta servizi di certificazione delle firme elettroniche o che fornisce altri servizi connessi con queste ultime;

h) chiave privata: l'elemento della coppia di chiavi asimmetriche, utilizzato dal soggetto titolare, mediante il quale si appone la firma digitale sul documento informatico;

i) chiave pubblica: l'elemento della coppia di chiavi asimmetriche destinato ad essere reso pubblico, con il quale si verifica la firma digitale apposta sul documento informatico dal titolare delle chiavi asimmetriche;

i-bis) copia informatica di documento analogico: il documento informatico avente contenuto identico a quello del documento analogico da cui è tratto;

i-ter) copia per immagine su supporto informatico di documento analogico: il documento informatico avente contenuto e forma identici a quelli del documento analogico da cui è tratto;

i-quater) copia informatica di documento informatico: il documento informatico avente contenuto identico a quello del documento da cui è tratto su supporto informatico con diversa sequenza di valori binari;

i-quinquies) duplicato informatico: il documento informatico ottenuto mediante la memorizzazione, sullo stesso dispositivo o su dispositivi diversi, della medesima sequenza di valori binari del documento originario;

l) dato a conoscibilità limitata: il dato la cui conoscibilità è riservata per legge o regolamento a specifici soggetti o categorie di soggetti;

m) dato delle pubbliche amministrazioni: il dato formato, o comunque trattato da una pubblica amministrazione;

n) dato pubblico: il dato conoscibile da chiunque;

o) disponibilità: la possibilità di accedere ai dati senza restrizioni non riconducibili a esplicite norme di legge;

p) documento informatico: la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti;

p-bis) documento analogico: la rappresentazione non informatica di atti, fatti o dati giuridicamente rilevanti;

q) firma elettronica: l'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di identificazione informatica;
q-bis) firma elettronica avanzata: insieme di dati in forma elettronica allegati oppure connessi a un documento informatico che consentono l'identificazione del firmatario del documento e garantiscono la connessione univoca al firmatario, creati con mezzi sui quali il firmatario può conservare un controllo esclusivo, collegati ai dati ai quali detta firma si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati;

r) firma elettronica qualificata: un particolare tipo di firma elettronica avanzata che sia basata su un certificato qualificato e realizzata mediante un dispositivo sicuro per la creazione della firma;

s) firma digitale: un particolare tipo di firma elettronica avanzata basata su un certificato qualificato e su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici;

t) fruibilità di un dato: la possibilità di utilizzare il dato anche trasferendolo nei sistemi informativi automatizzati di un'altra amministrazione;

u) gestione informatica dei documenti: l'insieme delle attività finalizzate alla registrazione e segnatura di protocollo, nonché alla classificazione, organizzazione, assegnazione, reperimento e conservazione dei documenti amministrativi formati o acquisiti dalle amministrazioni, nell'àmbito del sistema di classificazione d'archivio adottato, effettuate mediante sistemi informatici;
u-bis) gestore di posta elettronica certificata: il soggetto che presta servizi di trasmissione dei documenti informatici mediante la posta elettronica certificata;
"u-ter) identificazione informatica: la validazione dell'insieme di dati attribuiti in modo esclusivo ed univoco ad un soggetto, che ne consentono l'individuazione nei si-

stemi informativi, effettuata attraverso opportune tecnologie anche al fine di garantire la sicurezza dell'accesso;

v) originali non unici: i documenti per i quali sia possibile risalire al loro contenuto attraverso altre scritture o documenti di cui sia obbligatoria la conservazione, anche se in possesso di terzi;

v-bis) posta elettronica certificata: sistema di comunicazione in grado di attestare l'invio e l'avvenuta consegna di un messaggio di posta elettronica e di fornire ricevute opponibili ai terzi;

z) pubbliche amministrazioni centrali: le amministrazioni dello Stato, ivi compresi gli istituti e scuole di ogni ordine e grado e le istituzioni educative, le aziende ed amministrazioni dello Stato ad ordinamento autonomo, le istituzioni universitarie, gli enti pubblici non economici nazionali, l'Agenzia per la rappresentanza negoziale delle pubbliche amministrazioni (ARAN), le agenzie di cui al decreto legislativo 30 luglio 1999, n. 300;

aa) titolare: la persona fisica cui è attribuita la firma elettronica e che ha accesso ai dispositivi per la creazione della firma elettronica;

bb) validazione temporale: il risultato della procedura informatica con cui si attribuiscono, ad uno o più documenti informatici, una data ed un orario opponibili ai terzi.

2. *Finalità e àmbito di applicazione.*

1. Lo Stato, le regioni e le autonomie locali assicurano la disponibilità, la gestione, l'accesso, la trasmissione, la conservazione e la fruibilità dell'informazione in modalità digitale e si organizzano ed agiscono a tale fine utilizzando con le modalità più appropriate le tecnologie dell'informazione e della comunicazione.
2. ***Le disposizioni del presente codice si applicano alle pubbliche amministrazioni di cui all'articolo 1, comma 2, del decreto legislativo 30 marzo 2001, n. 165, nel rispetto del riparto di competenza di cui all'articolo 117 della Costituzione, nonché alle società, interamente partecipate da enti pubblici o con prevalente capitale pubblico inserite nel conto economico consolidato della pubblica amministrazione, come individuate dall'Istituto nazionale di statistica (I-***

STAT) ai sensi dell'articolo 1, comma 5, della legge 30 dicembre 2004, n. 311.

2-*bis*. Abrogato.

3. ***Le disposizioni di cui al capo II, agli articoli 40, 43 e 44 del Capo III, nonché al Capo IV, si applicano ai privati ai sensi dell'articolo 3 del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 e successive modificazioni.***
4. Le disposizioni di cui al capo V, concernenti l'accesso ai documenti informatici, e la fruibilità delle informazioni digitali si applicano anche ai gestori di servizi pubblici ed agli organismi di diritto pubblico.
5. Le disposizioni del presente codice si applicano nel rispetto della disciplina rilevante in materia di trattamento dei dati personali e, in particolare, delle disposizioni del codice in materia di protezione dei dati personali approvato con decreto legislativo 30 giugno 2003, n. 196. I cittadini e le imprese hanno, comunque, diritto ad ottenere che il trattamento dei dati effettuato mediante l'uso di tecnologie telematiche sia conformato al rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato.
6. Le disposizioni del presente codice non si applicano limitatamente all'esercizio delle attività e funzioni di ordine e sicurezza pubblica, difesa e sicurezza nazionale, e consultazioni elettorali. ***Con decreti del Presidente del Consiglio dei ministri, tenuto conto delle esigenze derivanti dalla natura delle proprie particolari funzioni, sono stabiliti le modalità, i limiti ed i tempi di applicazione delle disposizioni del presente Codice alla Presidenza del Consiglio dei Ministri, nonché all'Amministrazione economico-finanziaria***

Sezione II - Diritti dei cittadini e delle imprese

3. *Diritto all'uso delle tecnologie.*

1. I cittadini e le imprese hanno diritto a richiedere ed ottenere l'uso delle tecnologie telematiche nelle comunicazioni con le pubbliche amministrazioni, ***con i soggetti di cui all'articolo 2, com-***

ma 2, e con i gestori di pubblici servizi ai sensi di quanto previsto dal presente codice.

1-*bis*. Abrogato.

1-*ter*. La tutela giurisdizionale davanti al giudice amministrativo è disciplinata dal codice del processo amministrativo.

4. *Partecipazione al procedimento amministrativo informatico.*

1. La partecipazione al procedimento amministrativo e il diritto di accesso ai documenti amministrativi sono esercitabili mediante l'uso delle tecnologie dell'informazione e della comunicazione secondo quanto disposto dagli articoli 59 e 60 del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445.
2. Ogni atto e documento può essere trasmesso alle pubbliche amministrazioni con l'uso delle tecnologie dell'informazione e della comunicazione se formato ed inviato nel rispetto della vigente normativa.

5. Effettuazione dei pagamenti con modalità informatiche.

1. ***Le pubbliche amministrazioni consentono, sul territorio nazionale, l'effettuazione dei pagamenti ad esse spettanti, a qualsiasi titolo dovuti, fatte salve le attività di riscossione dei tributi regolate da specifiche normative, con l'uso delle tecnologie dell'informazione e della comunicazione.***
2. ***Le pubbliche amministrazioni centrali possono avvalersi, senza nuovi o maggiori oneri per la finanza pubblica, di prestatori di servizi di pagamento per consentire ai privati di effettuare i pagamenti in loro favore attraverso l'utilizzo di carte di debito, di credito o prepagate e di ogni altro strumento di pagamento elettronico disponibile. Il prestatore dei servizi di pagamento che riceve l'importo dell'operazione di pagamento, effettua il riversamento dell'importo trasferito al tesoriere dell'ente, registrando in apposito sistema informatico, a disposizione dell'amministrazione, il pagamento eseguito e la relativa causale, la corrispondenza di ciascun pagamento, i capitoli***

e gli articoli d'entrata oppure le contabilità speciali interessate.

3. *Con decreto del Ministro per la pubblica amministrazione e l'innovazione ed i Ministri competenti per materia, di concerto con il Ministro dell'economia e delle finanze, sentito DigitPA sono individuate le operazioni di pagamento interessate dai commi 1 e 2, i tempi da cui decorre la disposizione di cui al comma 1, le relative modalità per il riversamento, la rendicontazione da parte del prestatore dei servizi di pagamento e l'interazione tra i sistemi e i soggetti coinvolti nel pagamento, nonché il modello di convenzione che il prestatore di servizi di pagamento deve sottoscrivere per effettuare il servizio.*
4. *Le regioni, anche per quanto concerne i propri enti e le amministrazioni del Servizio sanitario nazionale, e gli enti locali adeguano i propri ordinamenti al principio di cui al comma 1.*

5-bis. Comunicazioni tra imprese e amministrazioni pubbliche.

1. *La presentazione di istanze, dichiarazioni, dati e lo scambio di informazioni e documenti, anche a fini statistici, tra le imprese e le amministrazioni pubbliche avviene esclusivamente utilizzando le tecnologie dell'informazione e della comunicazione. Con le medesime modalità le amministrazioni pubbliche adottano e comunicano atti e provvedimenti amministrativi nei confronti delle imprese.*
2. *Con decreto del Presidente del Consiglio dei Ministri, su proposta del Ministro per la pubblica amministrazione e l'innovazione, di concerto con il Ministro dello sviluppo economico e con il Ministro per la semplificazione normativa, sono adottate le modalità di attuazione del comma 1 da parte delle pubbliche amministrazioni centrali e fissati i relativi termini.*
3. *DigitPA, anche avvalendosi degli Uffici di cui all'articolo 17, provvede alla verifica dell'attuazione del comma 1 se-*

condo le modalità e i termini indicati nel decreto di cui al comma 2.

4. ***Il Governo promuove l'intesa con regioni ed enti locali in sede di Conferenza unificata per l'adozione degli indirizzi utili alla realizzazione delle finalità di cui al comma 1.***

6. *Utilizzo della posta elettronica certificata.*

1. **per le comunicazioni di cui all'articolo 48, comma 1, con i soggetti che hanno preventivamente dichiarato il proprio indirizzo ai sensi della vigente normativa tecnica, le pubbliche amministrazioni utilizzano la posta elettronica certificata. la dichiarazione dell'indirizzo vincola solo il dichiarante e rappresenta espressa accettazione dell'invio, tramite posta elettronica certificata, da parte delle pubbliche amministrazioni, degli atti e dei provvedimenti che lo riguardano.**

1-bis La consultazione degli indirizzi di posta elettronica certificata, di cui agli articoli 16, comma 10, e 16-bis, comma 5, del decreto-legge 29 novembre 2008, n. 185, convertito, con modificazioni, dalla legge 28 gennaio 2009, n. 2, e l'estrazione di elenchi dei suddetti indirizzi, da parte delle pubbliche amministrazioni è effettuata sulla base delle regole tecniche emanate da DigitPA, sentito il Garante per la protezione dei dati personali.

2. Abrogato.

2-bis. Abrogato.

7. *Qualità dei servizi resi e soddisfazione dell'utenza.*

1. Le pubbliche amministrazioni provvedono alla riorganizzazione ed aggiornamento dei servizi resi; a tale fine sviluppano l'uso delle tecnologie dell'informazione e della comunicazione, sulla base di una preventiva analisi delle reali esigenze dei cittadini e delle imprese, anche utilizzando strumenti per la valutazione del grado di soddisfazione degli utenti.

2. Entro il 31 maggio di ciascun anno le pubbliche amministrazioni centrali trasmettono al Ministro delegato per la funzione pubblica e al Ministro delegato per l'innovazione e le tecnologie una relazione sulla qualità dei servizi resi e sulla soddisfazione dell'utenza.

8. *Alfabetizzazione informatica dei cittadini.*

1. Lo Stato promuove iniziative volte a favorire l'alfabetizzazione informatica dei cittadini con particolare riguardo alle categorie a rischio di esclusione, anche al fine di favorire l'utilizzo dei servizi telematici delle pubbliche amministrazioni.

9. *Partecipazione democratica elettronica.*

1. ***Le pubbliche amministrazioni favoriscono*** ogni forma di uso delle nuove tecnologie per promuovere una maggiore partecipazione dei cittadini, anche residenti all'estero, al processo democratico e per facilitare l'esercizio dei diritti politici e civili sia individuali che collettivi.

10. ***Sportello unico per le attività produttive***

1. ***Lo sportello unico per le attività produttive di cui all'articolo 38, comma 3, del decreto-legge 25 giugno 2008, n.112, convertito, con modificazioni, dalla legge 6 agosto 2008, n.133, eroga i propri servizi verso l'utenza in via telematica.***
2. **Abrogato.**
3. **Abrogato.**
4. Lo Stato realizza, nell'àmbito di quanto previsto dal sistema pubblico di connettività di cui al presente decreto, un sistema informatizzato per le imprese relativo ai procedimenti di competenza delle amministrazioni centrali anche ai fini di quanto previsto all'articolo 11.

11. *Registro informatico degli adempimenti amministrativi per le imprese.*

1. Presso il Ministero delle attività produttive, che si avvale a questo scopo del sistema informativo delle camere di commercio, industria, artigianato e agricoltura, è istituito il Registro informatico degli adempimenti amministrativi per le imprese, di seguito denominato «Registro», il quale contiene l'elenco completo degli adempimenti amministrativi previsti dalle pubbliche amministrazioni per l'avvio e l'esercizio delle attività di impresa, nonché i dati raccolti dalle amministrazioni comunali negli archivi informatici di cui all'articolo 24, comma 2, del decreto legislativo 31 marzo 1998, n. 112. Il Registro, che si articola su base regionale con apposite sezioni del sito informatico, fornisce, ove possibile, il supporto necessario a compilare in via elettronica la relativa modulistica.
2. È fatto obbligo alle amministrazioni pubbliche, nonché ai concessionari di lavori e ai concessionari e gestori di servizi pubblici, di trasmettere in via informatica al Ministero delle attività produttive l'elenco degli adempimenti amministrativi necessari per l'avvio e l'esercizio dell'attività di impresa.
3. Con decreto del Presidente del Consiglio dei Ministri, su proposta del Ministro delle attività produttive e del Ministro delegato per l'innovazione e le tecnologie, sono stabilite le modalità di coordinamento, di attuazione e di accesso al Registro, nonché di connessione informatica tra le diverse sezioni del sito.
4. Il Registro è pubblicato su uno o più siti telematici, individuati con decreto del Ministro delle attività produttive.
5. Del Registro possono avvalersi le autonomie locali, qualora non provvedano in proprio, per i servizi pubblici da loro gestiti.
6. All'onere derivante dall'attuazione del presente articolo si provvede ai sensi dell'articolo 21, comma 2, della legge 29 luglio 2003, n. 229.

Sezione III - Organizzazione delle pubbliche amministrazioni rapporti fra Stato, regioni e autonomie locali

12. *Norme generali per l'uso delle tecnologie dell'informazione e delle comunicazioni nell'azione amministrativa.*

1. Le pubbliche amministrazioni nell'organizzare autonomamente la propria attività utilizzano le tecnologie dell'informazione e della comunicazione per la realizzazione degli obiettivi di efficienza, efficacia, economicità, imparzialità, trasparenza, semplificazione e partecipazione***, nonché per la garanzia dei diritti dei cittadini e delle imprese di cui al Capo I, sezione II, del presente decreto.***

1-*bis. Gli organi di governo nell'esercizio delle funzioni di indirizzo politico ed in particolare nell'emanazione delle direttive generali per l'attività amministrativa e per la gestione ai sensi del comma 1 dell'articolo 14 del decreto legislativo 30 marzo 2001, n. 165, e le amministrazioni pubbliche nella redazione del piano di performance di cui all'articolo 10 del decreto legislativo 27 ottobre 2009, n.150, dettano disposizioni per l'attuazione delle disposizioni del presente decreto.*

1-*ter*. I dirigenti rispondono dell'osservanza ed attuazione delle disposizioni di cui al presente decreto ai sensi e nei limiti degli articoli 21 e 55 del decreto legislativo 30 marzo 2001, n. 165, ferme restando le eventuali responsabilità penali, civili e contabili previste dalle norme vigenti. ***L'attuazione delle disposizioni del presente decreto è comunque rilevante ai fini della misurazione e valutazione della performance organizzativa ed individuale dei dirigenti.***

2. Le pubbliche amministrazioni adottano le tecnologie dell'informazione e della comunicazione nei rapporti interni, tra le diverse amministrazioni e tra queste e i privati, con misure informatiche, tecnologiche, e procedurali di sicurezza, secondo le regole tecniche di cui all'articolo 71.
3. Le pubbliche amministrazioni operano per assicurare l'uniformità e la graduale integrazione delle modalità di interazione degli utenti con i servizi informatici, ***ivi comprese le reti di telefonia fissa e mobile in tutte le loro articolazioni da esse erogati,*** qualunque sia il canale di erogazione, nel rispetto della autonomia e della specificità di ciascun erogatore di servizi.

4. Lo Stato promuove la realizzazione e l'utilizzo di reti telematiche come strumento di interazione tra le pubbliche amministrazioni ed i privati.
5. Le pubbliche amministrazioni utilizzano le tecnologie dell'informazione e della comunicazione, garantendo, nel rispetto delle vigenti normative, l'accesso alla consultazione, la circolazione e lo scambio di dati e informazioni, nonché l'interoperabilità dei sistemi e l'integrazione dei processi di servizio fra le diverse amministrazioni nel rispetto delle regole tecniche stabilite ai sensi dell'articolo 71.

5-*bis*. Le pubbliche amministrazioni implementano e consolidano i processi di informatizzazione in atto, ivi compresi quelli riguardanti l'erogazione ***attraverso le tecnologie dell'informazione e della comunicazione*** in via telematica di servizi a cittadini ed imprese anche con l'intervento di privati.

13. *Formazione informatica dei dipendenti pubblici.*

1. Le pubbliche amministrazioni nella predisposizione dei piani di cui all'articolo 7-bis, del decreto legislativo 30 marzo 2001, n. 165, e nell'àmbito delle risorse finanziarie previste dai piani medesimi, attuano anche politiche di formazione del personale finalizzate alla conoscenza e all'uso delle tecnologie dell'informazione e della comunicazione.

14. *Rapporti tra Stato, regioni e autonomie locali.*

1. In attuazione del disposto dell'articolo 117, secondo comma, lettera r), della Costituzione, lo Stato disciplina il coordinamento informatico dei dati dell'amministrazione statale, regionale e locale, dettando anche le regole tecniche necessarie per garantire la sicurezza e l'interoperabilità dei sistemi informatici e dei flussi informativi per la circolazione e lo scambio dei dati e per l'accesso ai servizi erogati in rete dalle amministrazioni medesime.
2. Lo Stato, le regioni e le autonomie locali promuovono le intese e gli accordi e adottano, attraverso la Conferenza unificata, gli indirizzi utili per realizzare un processo di digitalizzazione dell'azione

amministrativa coordinato e condiviso e per l'individuazione delle regole tecniche di cui all'articolo 71.

2-bis. Le regioni promuovono sul territorio azioni tese a realizzare un processo di digitalizzazione dell'azione amministrativa coordinato e condiviso tra le autonomie locali.

2-ter. Le regioni e gli enti locali digitalizzano la loro azione amministrativa e implementano l'utilizzo delle tecnologie dell'informazione e della comunicazione per garantire servizi migliori ai cittadini e alle imprese.

3. Lo Stato, ai fini di quanto previsto ai commi 1 e 2, istituisce organismi di cooperazione con le regioni e le autonomie locali, promuove intese ed accordi tematici e territoriali, favorisce la collaborazione interregionale, incentiva la realizzazione di progetti a livello locale, in particolare mediante il trasferimento delle soluzioni tecniche ed organizzative, previene il divario tecnologico tra amministrazioni di diversa dimensione e collocazione territoriale.

3-bis. Ai fini di quanto previsto ai commi 1, 2 e 3, è istituita senza nuovi o maggiori oneri per la finanza pubblica, presso la Conferenza unificata, previa delibera della medesima che ne definisce la composizione e le specifiche competenze, una Commissione permanente per l'innovazione tecnologica nelle regioni e negli enti locali con funzioni istruttorie e consultive.

15. *Digitalizzazione e riorganizzazione.*

1. La riorganizzazione strutturale e gestionale delle pubbliche amministrazioni volta al perseguimento degli obiettivi di cui all'articolo 12, comma 1, avviene anche attraverso il migliore e più esteso utilizzo delle tecnologie dell'informazione e della comunicazione nell'àmbito di una coordinata strategia che garantisca il coerente sviluppo del processo di digitalizzazione.
2. In attuazione del comma 1, le pubbliche amministrazioni provvedono in particolare a razionalizzare e semplificare i procedimenti amministrativi, le attività gestionali, i documenti, la modulistica, le modalità di accesso e di presentazione delle istanze da parte dei cittadini e delle imprese, assicurando che l'utilizzo delle tecnologie dell'informazione e della comunicazione avvenga in

conformità alle prescrizioni tecnologiche definite nelle regole tecniche di cui all'articolo 71.

2-*bis*. *Le Pubbliche amministrazioni nella valutazione dei progetti di investimento in materia di innovazione tecnologica tengono conto degli effettivi risparmi derivanti dalla razionalizzazione di cui al comma 2, nonché dei costi e delle economie che ne derivano.*

2-ter. Le Pubbliche amministrazioni, quantificano annualmente, ai sensi dell'articolo 27, del decreto legislativo 27 ottobre 2009, n.150, i risparmi effettivamente conseguiti in attuazione delle disposizioni di cui ai commi 1 e 2. Tali risparmi sono utilizzati, per due terzi secondo quanto previsto dall'articolo 27, comma 1, del citato decreto legislativo n. 150 del 2009 e in misura pari ad un terzo per il finanziamento di ulteriori progetti di innovazione.

3. La digitalizzazione dell'azione amministrativa è attuata dalle pubbliche amministrazioni con modalità idonee a garantire la partecipazione dell'Italia alla costruzione di reti transeuropee per lo scambio elettronico di dati e servizi fra le amministrazioni dei Paesi membri dell'Unione europea.

16. *Competenze del Presidente del Consiglio dei Ministri in materia di innovazione e tecnologie.*

1. Per il perseguimento dei fini di cui al presente codice, il Presidente del Consiglio dei Ministri o il Ministro delegato per l'innovazione e le tecnologie, nell'attività di coordinamento del processo di digitalizzazione e di coordinamento e di valutazione dei programmi, dei progetti e dei piani di azione formulati dalle pubbliche amministrazioni centrali per lo sviluppo dei sistemi informativi:

a) definisce con proprie direttive le linee strategiche, la pianificazione e le aree di intervento dell'innovazione tecnologica nelle pubbliche amministrazioni centrali, e ne verifica l'attuazione;

b) valuta, sulla base di criteri e metodiche di ottimizzazione della spesa, il corretto utilizzo delle risorse finanziarie per l'informatica e la telematica da parte delle singole amministrazioni centrali;

c) sostiene progetti di grande contenuto innovativo, di rilevanza strategica, di preminente interesse nazionale, con particolare attenzione per i progetti di carattere intersettoriale;
d) promuove l'informazione circa le iniziative per la diffusione delle nuove tecnologie;
e) detta norme tecniche ai sensi dell'articolo 71 e criteri in tema di pianificazione, progettazione, realizzazione, gestione, mantenimento dei sistemi informativi automatizzati delle pubbliche amministrazioni centrali e delle loro interconnessioni, nonché della loro qualità e relativi aspetti organizzativi e della loro sicurezza.

2. Il Presidente del Consiglio dei Ministri o il Ministro delegato per l'innovazione e le tecnologie riferisce annualmente al Parlamento sullo stato di attuazione del presente codice.

17. *Strutture per l'organizzazione, l'innovazione e le tecnologie.*

1. ***Le pubbliche amministrazioni centrali garantiscono l'attuazione delle linee strategiche per la riorganizzazione e digitalizzazione dell'amministrazione definite dal Governo. A tale fine, le predette amministrazioni individuano un unico ufficio dirigenziale generale, fermo restando il numero complessivo di tali Uffici, responsabile del coordinamento funzionale. Al predetto Ufficio afferiscono i compiti relativi a:***
   a) coordinamento strategico dello sviluppo dei sistemi informativi ***di telecomunicazione e fonia***, in modo da assicurare anche la coerenza con gli standard tecnici e organizzativi comuni;
   b) indirizzo e coordinamento dello sviluppo dei servizi, sia interni che esterni, forniti dai sistemi informativi ***di telecomunicazione e fonia*** dell'amministrazione;
   c) ***indirizzo, pianificazione, coordinamento e monitoraggio della sicurezza informatica relativamente ai dati, ai sistemi e alle infrastrutture anche in relazione al sistema pubblico di connettività, nel rispetto delle regole tecniche di cui all'articolo 51, comma 1;***

d) accesso dei soggetti disabili agli strumenti informatici e promozione dell'accessibilità anche in attuazione di quanto previsto dalla legge 9 gennaio 2004, n. 4;

e) analisi della coerenza tra l'organizzazione dell'amministrazione e l'utilizzo delle tecnologie dell'informazione e della comunicazione, al fine di migliorare la soddisfazione dell'utenza e la qualità dei servizi nonché di ridurre i tempi e i costi dell'azione amministrativa;

f) cooperazione alla revisione della riorganizzazione dell'amministrazione ai fini di cui alla lettera *e*);

g) indirizzo, coordinamento e monitoraggio della pianificazione prevista per lo sviluppo e la gestione dei sistemi informativi ***di telecomunicazione e fonia***;

h) progettazione e coordinamento delle iniziative rilevanti ai fini di una più efficace erogazione di servizi in rete a cittadini e imprese mediante gli strumenti della cooperazione applicativa tra pubbliche amministrazioni, ivi inclusa la predisposizione e l'attuazione di accordi di servizio tra amministrazioni per la realizzazione e compartecipazione dei sistemi informativi cooperativi;

i) promozione delle iniziative attinenti l'attuazione delle direttive impartite dal Presidente del Consiglio dei Ministri o dal Ministro delegato per l'innovazione e le tecnologie;

j) pianificazione e coordinamento del processo di diffusione, all'interno dell'amministrazione, dei sistemi di posta elettronica, protocollo informatico, firma digitale e mandato informatico, e delle norme in materia di accessibilità e fruibilità.

1-*bis. Per lo svolgimento dei compiti di cui al comma 1, le Agenzie, le Forze armate, compresa l'Arma dei carabinieri e il Corpo delle capitanerie di porto, nonché i Corpi di polizia hanno facoltà di individuare propri Uffici senza incrementare il numero complessivo di quelli già previsti nei rispettivi assetti organizzativi.*

1-*ter. DigitPA assicura il coordinamento delle iniziative di cui al comma 1, lettera c), con le modalità di cui all'articolo 51.*

18. *Conferenza permanente per l'innovazione tecnologica.*

1. È istituita la Conferenza permanente per l'innovazione tecnologica con funzioni di consulenza al Presidente del Consiglio dei Ministri, o al Ministro delegato per l'innovazione e le tecnologie, in materia di sviluppo ed attuazione dell'innovazione tecnologica nelle amministrazioni dello Stato.
2. La Conferenza permanente per l'innovazione tecnologica è presieduta da un rappresentante della Presidenza del Consiglio dei Ministri designato dal Presidente del Consiglio dei Ministri o dal Ministro delegato per l'innovazione e le tecnologie; ne fanno parte il Presidente del Centro nazionale per l'informatica nella pubblica amministrazione (d'ora in poi CNIPA), i componenti del CNIPA, il Capo del Dipartimento per l'innovazione e le tecnologie, nonché i responsabili delle funzioni di cui all'articolo 17.
3. La Conferenza permanente per l'innovazione tecnologica si riunisce con cadenza almeno semestrale per la verifica dello stato di attuazione dei programmi in materia di innovazione tecnologica e del piano triennale di cui all'articolo 9 del decreto legislativo 12 febbraio 1993, n. 39.
4. Il Presidente del Consiglio dei Ministri, o il Ministro delegato per l'innovazione e le tecnologie, provvede, con proprio decreto, a disciplinare il funzionamento della Conferenza permanente per l'innovazione tecnologica.
5. La Conferenza permanente per l'innovazione tecnologica può sentire le organizzazioni produttive e di categoria.
6. La Conferenza permanente per l'innovazione tecnologica opera senza rimborsi spese o compensi per i partecipanti a qualsiasi titolo dovuti, compreso il trattamento economico di missione; dal presente articolo non devono derivare nuovi o maggiori oneri per il bilancio dello Stato.

19. *Banca dati per la legislazione in materia di pubblico impiego.*

1. È istituita presso la Presidenza del Consiglio dei Ministri - Dipartimento della funzione pubblica, una banca dati contenente la normativa generale e speciale in materia di rapporto di lavoro alle dipendenze delle pubbliche amministrazioni.

2. La Presidenza del Consiglio dei Ministri - Dipartimento della funzione pubblica, cura l'aggiornamento periodico della banca dati di cui al comma 1, tenendo conto delle innovazioni normative e della contrattazione collettiva successivamente intervenuta, e assicurando agli utenti la consultazione gratuita.
3. All'onere derivante dall'attuazione del presente articolo si provvede ai sensi dell'articolo 21, comma 3, della legge 29 luglio 2003, n. 229.

Capo II - Documento informatico e firme elettroniche; pagamenti, libri e scritture

Sezione I - Documento informatico

20. *Documento informatico.*

1. Il documento informatico da chiunque formato, la ***memorizzazione*** su supporto informatico e la trasmissione con strumenti telematici conformi alle regole tecniche di cui all'articolo 71 sono validi e rilevanti agli effetti di legge, ai sensi delle disposizioni del presente codice.

1-bis. L'idoneità del documento informatico a soddisfare il requisito della forma scritta e il suo valore probatorio sono liberamente valutabili in giudizio, tenuto conto delle sue caratteristiche oggettive di qualità, sicurezza, integrità ed immodificabilità, fermo restando quanto disposto dall'articolo 21.

2. **Abrogato.**
3. ***Le regole tecniche per la formazione, per la trasmissione, la conservazione, la copia, la duplicazione, la riproduzione e la validazione temporale dei documenti informatici, nonché quelle in materia di generazione, apposizione e verifica di qualsiasi tipo di firma elettronica avanzata, sono stabilite ai sensi dell'articolo 71. La data e l'ora di formazione del documento informatico sono opponibili ai terzi se apposte in conformità alle regole tecniche sulla validazione temporale.***
4. Con le medesime regole tecniche sono definite le misure tecniche, organizzative e gestionali volte a garantire l'integrità, la di-

sponibilità e la riservatezza delle informazioni contenute nel documento informatico.

5. Restano ferme le disposizioni di legge in materia di protezione dei dati personali.

5-*bis.* *Gli obblighi di conservazione e di esibizione di documenti previsti dalla legislazione vigente si intendono soddisfatti a tutti gli effetti di legge a mezzo di documenti informatici, se le procedure utilizzate sono conformi alle regole tecniche dettate ai sensi dell'articolo 71.*

21. *Valore probatorio del documento informatico sottoscritto.*

1. Il documento informatico, cui è apposta una firma elettronica, sul piano probatorio è liberamente valutabile in giudizio, tenuto conto delle sue caratteristiche oggettive di qualità, sicurezza, integrità e immodificabilità.

2. Il documento informatico sottoscritto con firma elettronica avanzata, qualificata o digitale, formato nel rispetto delle regole tecniche di cui all'articolo 20, comma 3, che garantiscano l'identificabilità dell'autore, l'integrità e l'immodificabilità del documento, ha l'efficacia prevista dall'articolo 2702 del codice civile. L'utilizzo del dispositivo di firma si presume riconducibile al titolare, salvo che questi dia prova contraria.

2-bis). Salvo quanto previsto dall'articolo 25, le scritture private di cui all'articolo 1350, primo comma, numeri da 1 a 12, del codice civile, se fatte con documento informatico, sono sottoscritte, a pena di nullità, con firma elettronica qualificata o con firma digitale.

3. L'apposizione ad un documento informatico di una firma digitale o di un altro tipo di firma elettronica qualificata basata su un certificato elettronico revocato, scaduto o sospeso equivale a mancata sottoscrizione. La revoca o la sospensione, comunque motivate, hanno effetto dal momento della pubblicazione, salvo che il revocante, o chi richiede la sospensione, non dimostri che essa era già a conoscenza di tutte le parti interessate.

4. Le disposizioni del presente articolo si applicano anche se la firma elettronica è basata su un certificato qualificato rilasciato da un certificatore stabilito in uno Stato non facente parte dell'Unione europea, quando ricorre una delle seguenti condizioni:
   a) il certificatore possiede i requisiti di cui alla direttiva 1999/93/CE del 13 dicembre 1999 del Parlamento europeo e del Consiglio, ed è accreditato in uno Stato membro;
   b) il certificato qualificato è garantito da un certificatore stabilito nella Unione europea, in possesso dei requisiti di cui alla medesima direttiva;
   c) il certificato qualificato, o il certificatore, è riconosciuto in forza di un accordo bilaterale o multilaterale tra l'Unione europea e Paesi terzi o organizzazioni internazionali.
5. Gli obblighi fiscali relativi ai documenti informatici ed alla loro riproduzione su diversi tipi di supporto sono assolti secondo le modalità definite con uno o più decreti del Ministro dell'economia e delle finanze, sentito il Ministro delegato per l'innovazione e le tecnologie.

22. Copie informatiche di documenti analogici

1. ***I documenti informatici contenenti copia di atti pubblici, scritture private e documenti in genere, compresi gli atti e documenti amministrativi di ogni tipo formati in origine su supporto analogico, spediti o rilasciati dai depositari pubblici autorizzati e dai pubblici ufficiali, hanno piena efficacia, ai sensi degli articoli 2714 e 2715 del codice civile, se ad essi è apposta o associata, da parte di colui che li spedisce o rilascia, una firma digitale o altra firma elettronica qualificata. La loro esibizione e produzione sostituisce quella dell'originale.***
2. ***Le copie per immagine su supporto informatico di documenti originali formati in origine su supporto analogico hanno la stessa efficacia probatoria degli originali da cui sono estratte, se la loro conformità è attestata da un notaio o da altro pubblico ufficiale a ciò autorizzato, con dichiarazione allegata al documento informatico e asseverata secondo le regole tecniche stabilite ai sensi dell'articolo 71.***

3. Le copie per immagine su supporto informatico di documenti originali formati in origine su supporto analogico nel rispetto delle regole tecniche di cui all'articolo 71 hanno la stessa efficacia probatoria degli originali da cui sono tratte se la loro conformità all'originale non è espressamente disconosciuta.

4. Le copie formate ai sensi dei commi 1, 2 e 3 sostituiscono ad ogni effetto di legge gli originali formati in origine su supporto analogico, e sono idonee ad assolvere gli obblighi di conservazione previsti dalla legge, salvo quanto stabilito dal comma 5.

5. Con decreto del Presidente del Consiglio dei Ministri possono essere individuate particolari tipologie di documenti analogici originali unici per le quali, in ragione di esigenze di natura pubblicistica, permane l'obbligo della conservazione dell'originale analogico oppure, in caso di conservazione sostitutiva, la loro conformità all'originale deve essere autenticata da un notaio o da altro pubblico ufficiale a ciò autorizzato con dichiarazione da questi firmata digitalmente ed allegata al documento informatico.

6. Fino alla data di emanazione del decreto di cui al comma 5r per tutti i documenti analogici originali unici permane l'obbligo della conservazione dell'originale analogico oppure, in caso di conservazione sostitutiva, la loro conformità all'originale deve essere autenticata da un notaio o da altro pubblico ufficiale a ciò autorizzato con dichiarazione da questi firmata digitalmente ed allegata al documento informatico.

23. Copie analogiche di documenti informatici

1. Le copie su supporto analogico di documento informatico, anche sottoscritto con firma elettronica avanzata, qualificata o digitale, hanno la stessa efficacia probatoria dell'originale da cui sono tratte se la loro conformità all'originale in tutte le sue componenti è attestata da un pubblico ufficiale a ciò autorizzato.

2. Le copie e gli estratti su supporto analogico del documento informatico, conformi alle vigenti regole tecniche, hanno la stessa efficacia probatoria dell'originale se la loto conformità non è espressamente disconosciuta. Resta fermo, ove previsto l'obbligo di conservazione dell'originale informatico.

23-bis.- Duplicati e copie informatiche di documenti informatici

1. I duplicati informatici hanno il medesimo valore giuridico, ad ogni effetto di legge, del documento informatico da cui sono tratti, se prodotti in conformità alle regole tecniche di cui all'articolo 71.
2. Le copie e gli estratti informatici del documento informatico, se prodotti in conformità alle vigenti regole tecniche di cui all'articolo 71, hanno la stessa efficacia probatoria dell'originale da cui sono tratte se la loro conformità all'originale, in tutti le sue componenti, è attestata da un pubblico ufficiale a ciò autorizzato o se la conformità non è espressamente disconosciuta. Resta fermo, ove previsto, l'obbligo di conservazione dell'originale informatico.

23-ter. Documenti amministrativi informatici.

1. Gli atti formati dalle pubbliche amministrazioni con strumenti informatici, nonché i dati e i documenti informatici detenuti dalle stesse, costituiscono informazione primaria ed originale da cui è possibile effettuare, su diversi o identici tipi di supporto, duplicazioni e copie per gli usi consentiti dalla legge.
2. I documenti costituenti atti amministrativi con rilevanza interna al procedimento amministrativo sottoscritti con firma elettronica avanzata hanno l'efficacia prevista dall'art. 2702 del codice civile.
3. Le copie su supporto informatico di documenti formati dalla pubblica amministrazione in origine su supporto analogico ovvero da essa detenuti, hanno il medesimo valore giu-

ridico, ad ogni effetto di legge, degli originali da cui sono tratte, se la loro conformità all'originale è assicurata dal funzionario a ciò delegato nell'àmbito dell'ordinamento proprio dell'amministrazione di appartenenza, mediante l'utilizzo della firma digitale o di altra firma elettronica qualificata e nel rispetto delle regole tecniche stabilite ai sensi dell'articolo 71; in tale caso l'obbligo di conservazione dell'originale del documento è soddisfatto con la conservazione della copia su supporto informatico.

4. ***Le regole tecniche in materia di formazione e conservazione di documenti informatici delle pubbliche amministrazioni sono definite con decreto del Presidente del Consiglio dei Ministri o del Ministro delegato per la pubblica amministrazione e l'innovazione, di concerto con il Ministro per i beni e le attività culturali, nonché d'intesa con la Conferenza unificata di cui all'articolo 8 del decreto legislativo 28 agosto 1997, n. 281, e sentiti DigitPA e il Garante per la protezione dei dati personali.***
5. ***Al fine di assicurare la provenienza e la conformità all'originale, sulle copie analogiche di documenti informatici, è apposto a stampa, sulla base dei criteri definiti con linee guida emanate da DigitPA, un contrassegno generato elettronicamente, formato nel rispetto delle regole tecniche stabilite ai sensi dell'articolo 71 e tale da consentire la verifica automatica della conformità del documento analogico a quello informatico.***
6. ***Per quanto non previsto dal presente articolo si applicano gli articoli 21, 22 , 23 e 23-bis.***

23-quater. Riproduzioni informatiche.

1. ***All'articolo 2712 del codice civile dopo le parole: «riproduzioni fotografiche» è inserita la seguente: «, informatiche».".***

Sezione II - Firme elettroniche e certificatori

24. *Firma digitale*.

1. La firma digitale deve riferirsi in maniera univoca ad un solo soggetto ed al documento o all'insieme di documenti cui è apposta o associata.
2. L'apposizione di firma digitale integra e sostituisce l'apposizione di sigilli, punzoni, timbri, contrassegni e marchi di qualsiasi genere ad ogni fine previsto dalla normativa vigente.
3. Per la generazione della firma digitale deve adoperarsi un certificato qualificato che, al momento della sottoscrizione, non risulti scaduto di validità ovvero non risulti revocato o sospeso.
4. Attraverso il certificato qualificato si devono rilevare, secondo le regole tecniche stabilite ai sensi dell'articolo 71, la validità del certificato stesso, nonché gli elementi identificativi del titolare e del certificatore e gli eventuali limiti d'uso.

25. Firma autenticata.

1. ***Si ha per riconosciuta, ai sensi dell'articolo 2703 del codice civile, la firma elettronica o qualsiasi altro tipo di firma avanzata autenticata dal notaio o da altro pubblico ufficiale a ciò autorizzato.***
2. ***L'autenticazione della firma elettronica, anche mediante l'acquisizione digitale della sottoscrizione autografa, o di qualsiasi altro tipo di firma elettronica avanzata consiste nell'attestazione, da parte del pubblico ufficiale, che la firma è stata apposta in sua presenza dal titolare, previo accertamento della sua identità personale, della validità dell'eventuale certificato elettronico utilizzato e del fatto che il documento sottoscritto non è in contrasto con l'ordinamento giuridico.***
3. ***L'apposizione della firma digitale da parte del pubblico ufficiale ha l'efficacia di cui all'articolo 24, comma 2.***
4. ***Se al documento informatico autenticato deve essere allegato altro documento formato in originale su altro tipo di supporto, il pubblico ufficiale può allegare copia informati-***

ca autenticata dell'originale, secondo le disposizioni dell'articolo 23, comma 5.

26. *Certificatori.*

1. L'attività dei certificatori stabiliti in Italia o in un altro Stato membro dell'Unione europea è libera e non necessita di autorizzazione preventiva. Detti certificatori o, se persone giuridiche, i loro legali rappresentanti ed i soggetti preposti all'amministrazione, ***qualora emettano certificati qualificati,*** devono possedere i requisiti di onorabilità richiesti ai soggetti che svolgono funzioni di amministrazione, direzione e controllo presso le banche di cui all'articolo 26 del testo unico delle leggi in materia bancaria e creditizia, di cui al decreto legislativo 1° settembre 1993, n. 385, e successive modificazioni.
2. L'accertamento successivo dell'assenza o del venir meno dei requisiti di cui al comma 1 comporta il divieto di prosecuzione dell'attività intrapresa.
3. Ai certificatori qualificati e ai certificatori accreditati che hanno sede stabile in altri Stati membri dell'Unione europea non si applicano le norme del presente codice e le relative norme tecniche di cui all'articolo 71 e si applicano le rispettive norme di recepimento della direttiva 1999/93/CE.

27. *Certificatori qualificati.*

1. I certificatori che rilasciano al pubblico certificati qualificati devono trovarsi nelle condizioni previste dall'articolo 26.
2. I certificatori di cui al comma 1, devono inoltre:
   a) dimostrare l'affidabilità organizzativa, tecnica e finanziaria necessaria per svolgere attività di certificazione;
   b) utilizzare personale dotato delle conoscenze specifiche, dell'esperienza e delle competenze necessarie per i servizi forniti, in particolare della competenza a livello gestionale, della conoscenza specifica nel settore della tecnologia delle firme elettroniche e della dimestichezza con procedure di sicurezza ap-

propriate e che sia in grado di rispettare le norme del presente codice e le regole tecniche di cui all'articolo 71;

c) applicare procedure e metodi amministrativi e di gestione adeguati e conformi a tecniche consolidate;

d) utilizzare sistemi affidabili e prodotti di firma protetti da alterazioni e che garantiscano la sicurezza tecnica e crittografica dei procedimenti, in conformità a criteri di sicurezza riconosciuti in àmbito europeo e internazionale e certificati ai sensi dello schema nazionale di cui all'articolo 35, comma 5;

e) adottare adeguate misure contro la contraffazione dei certificati, idonee anche a garantire la riservatezza, l'integrità e la sicurezza nella generazione delle chiavi private nei casi in cui il certificatore generi tali chiavi.

3. I certificatori di cui al comma 1, devono comunicare, prima dell'inizio dell'attività, anche in via telematica, una dichiarazione di inizio di attività al CNIPA, attestante l'esistenza dei presupposti e dei requisiti previsti dal presente codice.
4. Il CNIPA procede, d'ufficio o su segnalazione motivata di soggetti pubblici o privati, a controlli volti ad accertare la sussistenza dei presupposti e dei requisiti previsti dal presente codice e dispone, se del caso, con provvedimento motivato da notificare all'interessato, il divieto di prosecuzione dell'attività e la rimozione dei suoi effetti, salvo che, ove ciò sia possibile, l'interessato provveda a conformare alla normativa vigente detta attività ed i suoi effetti entro il termine prefissatogli dall'amministrazione stessa.

28. *Certificati qualificati.*

1. I certificati qualificati devono contenere almeno le seguenti informazioni:
   a) indicazione che il certificato elettronico rilasciato è un certificato qualificato;
   b) numero di serie o altro codice identificativo del certificato;
   c) nome, ragione o denominazione sociale del certificatore che ha rilasciato il certificato e lo Stato nel quale è stabilito;
   d) nome, cognome o uno pseudonimo chiaramente identificato come tale e codice fiscale del titolare del certificato;

e) dati per la verifica della firma, cioè i dati peculiari, come codici o chiavi crittografiche pubbliche, utilizzati per verificare la firma elettronica corrispondenti ai dati per la creazione della stessa in possesso del titolare;
f) indicazione del termine iniziale e finale del periodo di validità del certificato;
g) firma elettronica del certificatore che ha rilasciato il certificato, realizzata in conformità alle regole tecniche ed idonea a garantire l'integrità e la veridicità di tutte le informazioni contenute nel certificato medesimo.

2. In aggiunta alle informazioni di cui al comma 1, fatta salva la possibilità di utilizzare uno pseudonimo, per i titolari residenti all'estero cui non risulti attribuito il codice fiscale, si deve indicare il codice fiscale rilasciato dall'autorità fiscale del Paese di residenza o, in mancanza, un analogo codice identificativo, quale ad esempio un codice di sicurezza sociale o un codice identificativo generale.
3. Il certificato qualificato può contenere, ove richiesto dal titolare o dal terzo interessato, le seguenti informazioni, se pertinenti allo scopo per il quale il certificato è richiesto:

a) le qualifiche specifiche del titolare, quali l'appartenenza ad ordini o collegi professionali, la qualifica di pubblico ufficiale, l'iscrizione ad albi o il possesso di altre abilitazioni professionali, nonché poteri di rappresentanza;
b) i limiti d'uso del certificato, inclusi quelli derivanti dalla titolarità delle qualifiche e dai poteri di rappresentanza di cui alla lettera *a*) ai sensi dell'articolo 30, comma 3.
c) limiti del valore degli atti unilaterali e dei contratti per i quali il certificato può essere usato, ove applicabili.

3-bis. Le informazioni di cui al comma 3 possono essere contenute in un separato certificato elettronico e possono essere rese disponibili anche in rete. Con decreto del Presidente del Consiglio dei Ministri sono definite le modalità di attuazione del presente comma, anche in riferimento alle pubbliche amministrazioni e agli ordini professionali.

4. Il titolare, ovvero il terzo interessato se richiedente ai sensi del comma 3, comunicano tempestivamente al certificatore il modi-

ficarsi o venir meno delle circostanze oggetto delle informazioni di cui al presente articolo.

29. *Accreditamento.*

1. I certificatori che intendono conseguire il riconoscimento del possesso dei requisiti del livello più elevato, in termini di qualità e di sicurezza, chiedono di essere accreditati presso il CNIPA.
2. Il richiedente deve rispondere ai requisiti di cui all'articolo 27, ed allegare alla domanda oltre ai documenti indicati nel medesimo articolo il profilo professionale del personale responsabile della generazione dei dati per la creazione e per la verifica della firma, della emissione dei certificati e della gestione del registro dei certificati nonché l'impegno al rispetto delle regole tecniche.
3. Il richiedente, se soggetto privato, in aggiunta a quanto previsto dal comma 2, deve inoltre:
   a) avere forma giuridica di società di capitali e un capitale sociale non inferiore a quello necessario ai fini dell'autorizzazione alla attività bancaria ai sensi dell'articolo 14 del testo unico delle leggi in materia bancaria e creditizia, di cui al decreto legislativo 1° settembre 1993, n. 385;
   b) garantire il possesso, oltre che da parte dei rappresentanti legali, anche da parte dei soggetti preposti alla amministrazione e dei componenti degli organi preposti al controllo, dei requisiti di onorabilità richiesti ai soggetti che svolgono funzioni di amministrazione, direzione e controllo presso banche ai sensi dell'articolo 26 del decreto legislativo 1° settembre 1993, n. 385.
4. La domanda di accreditamento si considera accolta qualora non venga comunicato all'interessato il provvedimento di diniego entro novanta giorni dalla data di presentazione della stessa.
5. Il termine di cui al comma 4, può essere sospeso una sola volta entro trenta giorni dalla data di presentazione della domanda, esclusivamente per la motivata richiesta di documenti che integrino o completino la documentazione presentata e che non siano già nella disponibilità del CNIPA o che questo non possa acquisire autonomamente. In tale caso, il termine riprende a decorrere dalla data di ricezione della documentazione integrativa.

6. A seguito dell'accoglimento della domanda, il CNIPA dispone l'iscrizione del richiedente in un apposito elenco pubblico, tenuto dal CNIPA stesso e consultabile anche in via telematica, ai fini dell'applicazione della disciplina in questione.
7. Il certificatore accreditato può qualificarsi come tale nei rapporti commerciali e con le pubbliche amministrazioni.
8. ***Il valore giuridico delle firme elettroniche qualificate e delle firme digitali basate su certificati qualificati rilasciati da certificatori accreditati in altri Stati membri dell'Unione europea ai sensi dell'articolo 3, paragrafo 2, della direttiva 1999/93/CE è equiparato a quello previsto per le firme elettroniche qualificate e per le firme digitali basate su certificati qualificati emessi dai certificatori accreditati ai sensi del presente articolo.***
9. Alle attività previste dal presente articolo si fa fronte nell'àmbito delle risorse del CNIPA, senza nuovi o maggiori oneri per la finanza pubblica.

30. *Responsabilità del certificatore.*

1. Il certificatore che rilascia al pubblico un certificato qualificato o che garantisce al pubblico l'affidabilità del certificato è responsabile, se non prova d'aver agito senza colpa o dolo, del danno cagionato a chi abbia fatto ragionevole affidamento:
   a) sull'esattezza e sulla completezza delle informazioni necessarie alla verifica della firma in esso contenute alla data del rilascio e sulla loro completezza rispetto ai requisiti fissati per i certificati qualificati;
   b) sulla garanzia che al momento del rilascio del certificato il firmatario detenesse i dati per la creazione della firma corrispondenti ai dati per la verifica della firma riportati o identificati nel certificato;
   c) sulla garanzia che i dati per la creazione e per la verifica della firma possano essere usati in modo complementare, nei casi in cui il certificatore generi entrambi;
   d) sull'adempimento degli obblighi a suo carico previsti dall'articolo 32.

2. Il certificatore che rilascia al pubblico un certificato qualificato è responsabile, nei confronti dei terzi che facciano affidamento sul certificato stesso, dei danni provocati per effetto della mancata o non tempestiva registrazione della revoca o non tempestiva sospensione del certificato, secondo quanto previsto. dalle regole tecniche di cui all'articolo 71, salvo che provi d'aver agito senza colpa.
3. Il certificato qualificato può contenere limiti d'uso ovvero un valore limite per i negozi per i quali può essere usato il certificato stesso, purché i limiti d'uso o il valore limite siano riconoscibili da parte dei terzi e siano chiaramente evidenziati nel certificato secondo quanto previsto dalle regole tecniche di cui all'articolo 71. Il certificatore non è responsabile dei danni derivanti dall'uso di un certificato qualificato che ecceda i limiti posti dallo stesso o derivanti dal superamento del valore limite.

Art. 31. Vigilanza sull'attività dei certificatori e dei gestori di posta elettronica certificata

1. DigitPA svolge funzioni di vigilanza e controllo sull'attività dei certificatori qualificati e dei gestori di posta elettronica certificata.

32. *Obblighi del titolare e del certificatore.*

1. Il titolare del certificato di firma è tenuto ad assicurare la custodia del dispositivo di forma e ad adottare tutte le misure organizzative e tecniche idonee ad evitare danno ad altri; è altresì tenuto ad utilizzare personalmente il dispositivo di firma.
2. Il certificatore è tenuto ad adottare tutte le misure organizzative e tecniche idonee ad evitare danno a terzi.
3. Il certificatore che rilascia, ai sensi dell'articolo 19, certificati qualificati deve inoltre:
   a) provvedere con certezza alla identificazione della persona che fa richiesta della certificazione;
   b) rilasciare e rendere pubblico il certificato elettronico nei modi o nei casi stabiliti dalle regole tecniche di cui all'articolo 71,

nel rispetto del decreto legislativo 30 giugno 2003, n. 196, e successive modificazioni;

c) specificare, nel certificato qualificato su richiesta dell'istante, e con il consenso del terzo interessato, i poteri di rappresentanza o altri titoli relativi all'attività professionale o a cariche rivestite, previa verifica della documentazione presentata dal richiedente che attesta la sussistenza degli stessi;

d) attenersi alle regole tecniche di cui all'articolo 71;

e) informare i richiedenti in modo compiuto e chiaro, sulla procedura di certificazione e sui necessari requisiti tecnici per accedervi e sulle caratteristiche e sulle limitazioni d'uso delle firme emesse sulla base del servizio di certificazione;

f) (soppressa);

g) procedere alla tempestiva pubblicazione della revoca e della sospensione del certificato elettronico in caso di richiesta da parte del titolare o del terzo dal quale derivino i poteri del titolare medesimo, di perdita del possesso o della compromissione del dispositivo di firma, di provvedimento dell'autorità, di acquisizione della conoscenza di cause limitative della capacità del titolare, di sospetti abusi o falsificazioni, secondo quanto previsto dalle regole tecniche di cui all'articolo 71;

h) garantire un servizio di revoca e sospensione dei certificati elettronici sicuro e tempestivo nonché garantire il funzionamento efficiente, puntuale e sicuro degli elenchi dei certificati di firma emessi, sospesi e revocati;

i) assicurare la precisa determinazione della data e dell'ora di rilascio, di revoca e di sospensione dei certificati elettronici;

j) tenere registrazione, anche elettronica, di tutte le informazioni relative al certificato qualificato dal momento della sua emissione almeno per venti anni anche al fine di fornire prova della certificazione in eventuali procedimenti giudiziari;

k) non copiare, né conservare, le chiavi private di firma del soggetto cui il certificatore ha fornito il servizio di certificazione;

l) predisporre su mezzi di comunicazione durevoli tutte le informazioni utili ai soggetti che richiedono il servizio di certificazione, tra cui in particolare gli esatti termini e condizioni relative all'uso del certificato, compresa ogni limitazione dell'uso, l'esistenza di un sistema di accreditamento facoltativo e le

procedure di reclamo e di risoluzione delle controversie; dette informazioni, che possono essere trasmesse elettronicamente, devono essere scritte in linguaggio chiaro ed essere fornite prima dell'accordo tra il richiedente il servizio ed il certificatore;

m) utilizzare sistemi affidabili per la gestione del registro dei certificati con modalità tali da garantire che soltanto le persone autorizzate possano effettuare inserimenti e modifiche, che l'autenticità delle informazioni sia verificabile, che i certificati siano accessibili alla consultazione del pubblico soltanto nei casi consentiti dal titolare del certificato e che l'operatore possa rendersi conto di qualsiasi evento che comprometta i requisiti di sicurezza. Su richiesta, elementi pertinenti delle informazioni possono essere resi accessibili a terzi che facciano affidamento sul certificato.

m-bis) garantire il corretto funzionamento e la continuità del sistema e comunicare immediatamente a DigitPA e agli utenti eventuali malfunzionamenti che determinano disservizio, sospensione o interruzione del servizio stesso.

4. Il certificatore è responsabile dell'identificazione del soggetto che richiede il certificato qualificato di firma anche se tale attività è delegata a terzi.
5. Il certificatore raccoglie i dati personali solo direttamente dalla persona cui si riferiscono o previo suo esplicito consenso, e soltanto nella misura necessaria al rilascio e al mantenimento del certificato, fornendo l'informativa prevista dall'articolo 13 del decreto legislativo 30 giugno 2003, n. 196. I dati non possono essere raccolti o elaborati per fini diversi senza l'espresso consenso della persona cui si riferiscono

33. *Uso di pseudonimi.*

1. In luogo del nome del titolare il certificatore può riportare sul certificato elettronico uno pseudonimo, qualificandolo come tale. Se il certificato è qualificato, il certificatore ha l'obbligo di conservare le informazioni relative alla reale identità del titolare per almeno ***venti anni decorrenti dall'emissione*** del certificato stesso.

34. *Norme particolari per le pubbliche amministrazioni e per altri soggetti qualificati.*

1. Ai fini della sottoscrizione, ove prevista, di documenti informatici di rilevanza esterna, le pubbliche amministrazioni:
   a) possono svolgere direttamente l'attività di rilascio dei certificati qualificati avendo a tale fine l'obbligo di accreditarsi ai sensi dell'articolo 29; tale attività può essere svolta esclusivamente nei confronti dei propri organi ed uffici, nonché di categorie di terzi, pubblici o privati. I certificati qualificati rilasciati in favore di categorie di terzi possono essere utilizzati soltanto nei rapporti con l'Amministrazione certificante, al di fuori dei quali sono privi di ogni effetto ad esclusione di quelli rilasciati da collegi e ordini professionali e relativi organi agli iscritti nei rispettivi albi e registri; con decreto del Presidente del Consiglio dei Ministri, su proposta dei Ministri per la funzione pubblica e per l'innovazione e le tecnologie e dei Ministri interessati, di concerto con il Ministro dell'economia e delle finanze, sono definite le categorie di terzi e le caratteristiche dei certificati qualificati;
   b) possono rivolgersi a certificatori accreditati, secondo la vigente normativa in materia di contratti pubblici.
2. Per la formazione, gestione e sottoscrizione di documenti informatici aventi rilevanza esclusivamente interna ciascuna amministrazione può adottare, nella propria autonomia organizzativa, regole diverse da quelle contenute nelle regole tecniche di cui all'articolo 71.
3. Le regole tecniche concernenti la qualifica di pubblico ufficiale, l'appartenenza ad ordini o collegi professionali, l'iscrizione ad albi o il possesso di altre abilitazioni sono emanate con decreti di cui all'articolo 71 di concerto con il Ministro per la funzione pubblica, con il Ministro della giustizia e con gli altri Ministri di volta in volta interessati, sulla base dei princìpi generali stabiliti dai rispettivi ordinamenti.
4. Nelle more della definizione delle specifiche norme tecniche di cui al comma 3, si applicano le norme tecniche vigenti in materia di firme digitali.

5. Entro ventiquattro mesi dalla data di entrata in vigore del presente codice le pubbliche amministrazioni devono dotarsi di idonee procedure informatiche e strumenti software per la verifica delle firme digitali secondo quanto previsto dalle regole tecniche di cui all'articolo 71.

35. *Dispositivi sicuri e procedure per la generazione della firma.*

1. I dispositivi sicuri e le procedure utilizzate per la generazione delle firme devono presentare requisiti di sicurezza tali da garantire che la chiave privata:
   a) sia riservata;
   b) non possa essere derivata e che la relativa firma sia protetta da contraffazioni;
   c) possa essere sufficientemente protetta dal titolare dall'uso da parte di terzi.
2. I dispositivi sicuri e le procedure di cui al comma 1 devono garantire l'integrità dei documenti informatici a cui la firma si riferisce. I documenti informatici devono essere presentati al titolare, prima dell'apposizione della firma, chiaramente e senza ambiguità, e si deve richiedere conferma della volontà di generare la firma secondo quanto previsto dalle regole tecniche di cui all'articolo 71.
3. ***Il secondo periodo del comma 2 non si applica alle firme apposte con procedura automatica. La firma con procedura automatica è valida se apposta previo consenso del titolare all'adozione della procedura medesima.***
4. ***I dispositivi sicuri di firma devono essere dotati di certificazione di sicurezza ai sensi dello schema nazionale di cui al comma 5.***
5. La conformità dei requisiti di sicurezza dei dispositivi per la creazione di una firma qualificata prescritti dall'allegato III della direttiva 1999/93/CE è accertata, in Italia ***dall'Organismo di certificazione della sicurezza informatica***, in base allo schema nazionale per la valutazione e certificazione di sicurezza nel settore della tecnologia dell'informazione, fissato con decreto del Presidente del Consiglio dei Ministri, o, per sua delega, del Ministro per l'innovazione e le tecnologie, di concerto con i Ministri

delle comunicazioni, delle attività produttive e dell'economia e delle finanze. ***L'attuazione dello schema nazionale non deve determinare nuovi o maggiori oneri per il bilancio dello Stato.*** Lo schema nazionale può prevedere altresì la valutazione e la certificazione relativamente ad ulteriori criteri europei ed internazionali, anche riguardanti altri sistemi e prodotti afferenti al settore suddetto.

6. ***La conformità di cui al comma 5 è inoltre riconosciuta se accertata da un organismo all'uopo designato da un altro Stato membro e notificato ai sensi dell'articolo 11, paragrafo 1, lettera b), della direttiva 1999/93/CE***.

36. *Revoca e sospensione dei certificati qualificati.*

1. Il certificato qualificato deve essere a cura del certificatore:
   a) revocato in caso di cessazione dell'attività del certificatore salvo quanto previsto dal comma 2 dell'articolo 37;
   b) revocato o sospeso in esecuzione di un provvedimento dell'autorità;
   c) revocato o sospeso a seguito di richiesta del titolare o del terzo dal quale derivano i poteri del titolare, secondo le modalità previste nel presente codice;
   d) revocato o sospeso in presenza di cause limitative della capacità del titolare o di abusi o falsificazioni.
2. Il certificato qualificato può, inoltre, essere revocato o sospeso nei casi previsti dalle regole tecniche di cui all'articolo 71.
3. La revoca o la sospensione del certificato qualificato, qualunque ne sia la causa, ha effetto dal momento della pubblicazione della lista che lo contiene. Il momento della pubblicazione deve essere attestato mediante adeguato riferimento temporale.
4. Le modalità di revoca o sospensione sono previste nelle regole tecniche di cui all'articolo 71.

37. *Cessazione dell'attività.*

1. Il certificatore qualificato o accreditato che intende cessare l'attività deve, almeno sessanta giorni prima della data di cessazione, darne avviso al CNIPA e informare senza indugio i titolari dei certificati da lui emessi specificando che tutti i certificati non scaduti al momento della cessazione saranno revocati.
2. Il certificatore di cui al comma 1 comunica contestualmente la rilevazione della documentazione da parte di altro certificatore o l'annullamento della stessa. L'indicazione di un certificatore sostitutivo evita la revoca di tutti i certificati non scaduti al momento della cessazione.
3. Il certificatore di cui al comma 1 indica altro depositario del registro dei certificati e della relativa documentazione.
4. Il CNIPA rende nota la data di cessazione dell'attività del certificatore accreditato tramite l'elenco di cui all'articolo 29, comma 6.

4-bis. Qualora il certificatore qualificato cessi la propria attività senza indicare, ai sensi del comma 2, un certificatore sostitutivo e non si impegni a garantire la conservazione e la disponibilità della documentazione prevista dagli articoli 33 e 32, comma 3, lettera j) e delle ultime liste di revoca emesse, deve provvedere al deposito presso DigitPA che ne garantisce la conservazione e la disponibilità.

Sezione III - ***Trasferimenti di fondi***, libri e scritture

38. ***Trasferimenti di fondi***.

1. Il trasferimento in via telematica di fondi tra pubbliche amministrazioni e tra queste e soggetti privati è effettuato secondo le regole tecniche stabilite ai sensi dell'articolo 71 di concerto con i Ministri per la funzione pubblica, della giustizia e dell'economia e delle finanze, sentiti il Garante per la protezione dei dati personali e la Banca d'Italia.

39. *Libri e scritture.*

1. I libri, i repertori e le scritture, ivi compresi quelli previsti dalla legge sull'ordinamento del notariato e degli archivi notarili, di cui

sia obbligatoria la tenuta possono essere formati e conservati su supporti informatici in conformità alle disposizioni del presente codice e secondo le regole tecniche stabilite ai sensi dell'articolo 71.

Capo III - Formazione, gestione e conservazione dei documenti informatici

40. *Formazione di documenti informatici.*

1. Le pubbliche amministrazioni formano gli originali dei propri documenti con mezzi informatici secondo le disposizioni di cui al presente codice e le regole tecniche di cui all'articolo 71.
2. ***Abrogato***
3. Con apposito regolamento, da emanarsi entro 180 giorni dalla data di entrata in vigore del presente codice, ai sensi dell'articolo 17, comma 1, della legge 23 agosto 1988, n. 400, sulla proposta dei Ministri delegati per la funzione pubblica, per l'innovazione e le tecnologie e del Ministro per i beni e le attività culturali, sono individuate le categorie di documenti amministrativi che possono essere redatti in originale anche su supporto cartaceo in relazione al particolare valore di testimonianza storica ed archivistica che sono idonei ad assumere.
4. Il Presidente del Consiglio dei Ministri, con propri decreti, fissa la data dalla quale viene riconosciuto il valore legale degli albi, elenchi, pubblici registri ed ogni altra raccolta di dati concernenti stati, qualità personali e fatti già realizzati dalle amministrazioni, su supporto informatico, in luogo dei registri cartacei.

40-bis. Protocollo informatico.

1. ***Formano comunque oggetto di registrazione di protocollo ai sensi dell'articolo 53 del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, le comunicazioni che pervengono o sono inviate dalle caselle di posta elettronica***

di cui agli articoli 47, commi 1 e 3, 54, comma 2-ter e 57-bis, comma 1, nonché le istanze e le dichiarazioni di cui all'articolo 65 in conformità alle regole tecniche di cui all'articolo 71.

41. *Procedimento e fascicolo informatico.*

1. Le pubbliche amministrazioni gestiscono i procedimenti amministrativi utilizzando le tecnologie dell'informazione e della comunicazione, nei casi e nei modi previsti dalla normativa vigente.

1-bis. La gestione dei procedimenti amministrativi è attuata in modo da consentire, mediante strumenti automatici, il rispetto di quanto previsto all'articolo 54, commi 2-ter e 2-quater.

2. La pubblica amministrazione titolare del procedimento ***raccoglie*** in un fascicolo informatico gli atti, i documenti e i dati del procedimento medesimo da chiunque formati; all'atto della comunicazione dell'avvio del procedimento ai sensi dell'articolo 8 della legge 7 agosto 1990, n. 241, comunica agli interessati le modalità per esercitare in via telematica i diritti di cui all'articolo 10 della citata legge 7 agosto 1990, n. 241.

2-*bis*. Il fascicolo informatico è realizzato garantendo la possibilità di essere direttamente consultato ed alimentato da tutte le amministrazioni coinvolte nel procedimento. Le regole per la costituzione***, l'identificazione*** e l'utilizzo del fascicolo sono conformi ai principi di una corretta gestione documentale ed alla disciplina della formazione, gestione, conservazione e trasmissione del documento informatico, ivi comprese le regole concernenti il protocollo informatico ed il sistema pubblico di connettività, e comunque rispettano i criteri dell'interoperabilità e della cooperazione applicativa; regole tecniche specifiche possono essere dettate ai sensi dell'articolo 71, di concerto con il Ministro della funzione pubblica.

2-*ter*. Il fascicolo informatico reca l'indicazione:

a) dell'amministrazione titolare del procedimento, che cura la costituzione e la gestione del fascicolo medesimo;
b) delle altre amministrazioni partecipanti;
c) del responsabile del procedimento;

d) dell'oggetto del procedimento;
e) dell'elenco dei documenti contenuti, salvo quanto disposto dal comma 2-*quater*.
e-bis) dell'identificativo del fascicolo medesimo.

2-*quater*. Il fascicolo informatico può contenere aree a cui hanno accesso solo l'amministrazione titolare e gli altri soggetti da essa individuati; esso è formato in modo da garantire la corretta collocazione, la facile reperibilità e la collegabilità, in relazione al contenuto ed alle finalità, dei singoli documenti; è inoltre costituito in modo da garantire l'esercizio in via telematica dei diritti previsti dalla citata legge n. 241 del 1990.

3. Ai sensi degli articoli da 14 a 14-*quinquies* della legge 7 agosto 1990, n. 241, previo accordo tra le amministrazioni coinvolte, la conferenza dei servizi è convocata e svolta avvalendosi degli strumenti informatici disponibili, secondo i tempi e le modalità stabiliti dalle amministrazioni medesime.

42. *Dematerializzazione dei documenti delle pubbliche amministrazioni.*

1. Le pubbliche amministrazioni valutano in termini di rapporto tra costi e benefici il recupero su supporto informatico dei documenti e degli atti cartacei dei quali sia obbligatoria o opportuna la conservazione e provvedono alla predisposizione dei conseguenti piani di sostituzione degli archivi cartacei con archivi informatici, nel rispetto delle regole tecniche adottate ai sensi dell'articolo 71.

43. *Riproduzione e conservazione dei documenti.*

1. I documenti degli archivi, le scritture contabili, la corrispondenza ed ogni atto, dato o documento di cui è prescritta la conservazione per legge o regolamento, ove riprodotti su supporti informatici sono validi e rilevanti a tutti gli effetti di legge, se ***la riproduzione e la conservazione nel tempo sono effettuate*** in modo da garantire la conformità dei documenti agli originali, nel rispetto delle regole tecniche stabilite ai sensi dell'articolo 71.

2. Restano validi i documenti degli archivi, le scritture contabili, la corrispondenza ed ogni atto, dato o documento già conservati mediante riproduzione su supporto fotografico, su supporto ottico o con altro processo idoneo a garantire la conformità dei documenti agli originali.
3. I documenti informatici, di cui è prescritta la conservazione per legge o regolamento, possono essere archiviati per le esigenze correnti anche con modalità cartacee e sono conservati in modo permanente con modalità digitali***, nel rispetto delle regole tecniche stabilite ai sensi dell'articolo 71.***
4. Sono fatti salvi i poteri di controllo del Ministero per i beni e le attività culturali sugli archivi delle pubbliche amministrazioni e sugli archivi privati dichiarati di notevole interesse storico ai sensi delle disposizioni del decreto legislativo 22 gennaio 2004, n. 42

44. *Requisiti per la conservazione dei documenti informatici.*

1. Il sistema di conservazione dei documenti informatici ***assicura***:
   a) l'identificazione certa del soggetto che ha formato il documento e dell'amministrazione o dell'area organizzativa omogenea di riferimento di cui all'articolo 50, comma 4, del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445;
   b) l'integrità del documento;
   c) la leggibilità e l'agevole reperibilità dei documenti e delle informazioni identificative, inclusi i dati di registrazione e di classificazione originari;
   d) il rispetto delle misure di sicurezza previste dagli articoli da 31 a 36 del decreto legislativo 30 giugno 2003, n. 196, e dal disciplinare tecnico pubblicato in allegato B a tale decreto.

1-bis. Il sistema di conservazione dei documenti informatici è gestito da un responsabile che opera d'intesa con il responsabile del trattamento dei dati personali di cui all'articolo 29 del decreto legislativo 30 giugno 2003, n. 196, e, ove previsto, con il responsabile del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi di cui all'articolo 61 del decreto del Presidente della Repubblica 28

dicembre 2000, n. 445, nella definizione e gestione delle attività di rispettiva competenza.

1-ter. Il responsabile della conservazione può chiedere la conservazione dei documenti informatici o la certificazione della conformità del relativo processo di conservazione a quanto stabilito dall'articolo 43 e dalle regole tecniche ivi previste, nonché dal comma 1 ad altri soggetti, pubblici o privati, che offrono idonee garanzie organizzative e tecnologiche.

44-bis. Conservatori accreditati

1. ***I soggetti pubblici e privati che svolgono attività di conservazione dei documenti informatici e di certificazione dei relativi processi anche per conto di terzi ed intendono conseguire il riconoscimento del possesso dei requisiti del livello più elevato, in termini di qualità e di sicurezza, chiedono l'accreditamento presso DigitPA.***
2. ***Si applicano, in quanto compatibili, gli articoli 26, 27, 29, ad eccezione del comma 3, lettera a) e 31.***
3. ***I soggetti privati di cui al comma 1 sono costituiti in società di capitali con capitale sociale non inferiore a euro 200.000.***

Capo IV - Trasmissione informatica dei documenti

45. *Valore giuridico della trasmissione.*

1. I documenti trasmessi da chiunque ad una pubblica amministrazione con qualsiasi mezzo telematico o informatico, idoneo ad accertarne la fonte di provenienza, soddisfano il requisito della forma scritta e la loro trasmissione non deve essere seguita da quella del documento originale.
2. Il documento informatico trasmesso per via telematica si intende spedito dal mittente se inviato al proprio gestore, e si intende consegnato al destinatario se reso disponibile all'indirizzo elet-

tronico da questi dichiarato, nella casella di posta elettronica del destinatario messa a disposizione dal gestore.

46. *Dati particolari contenuti nei documenti trasmessi.*

1. Al fine di garantire la riservatezza dei dati sensibili o giudiziari di cui all'articolo 4, comma 1, lettere d) ed e), del decreto legislativo 30 giugno 2003, n. 196, i documenti informatici trasmessi ad altre pubbliche amministrazioni per via telematica possono contenere soltanto le informazioni relative a stati, fatti e qualità personali previste da legge o da regolamento e indispensabili per il perseguimento delle finalità per le quali sono acquisite.

47. *Trasmissione dei documenti attraverso la posta elettronica tra le pubbliche amministrazioni.*

1. Le comunicazioni di documenti tra le pubbliche amministrazioni avvengono mediante l'utilizzo della posta elettronica ***o in cooperazione applicativa***; esse sono valide ai fini del procedimento amministrativo una volta che ne sia verificata la provenienza.
2. Ai fini della verifica della provenienza le comunicazioni sono valide se:
   a) sono sottoscritte con firma digitale o altro tipo di firma elettronica qualificata;
   b) ovvero sono dotate di ***segnatura di protocollo di cui all'articolo 55 del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445***;
   c) ovvero è comunque possibile accertarne altrimenti la provenienza, secondo quanto previsto dalla normativa vigente o dalle regole tecniche di cui all'articolo 71;
   d) ovvero trasmesse attraverso sistemi di posta elettronica certificata di cui al decreto del Presidente della Repubblica 11 febbraio 2005, n. 68.
3. ***Le pubbliche amministrazioni e gli altri soggetti di cui all'articolo 2, comma 2, provvedono ad istituire e pubblicare nell'Indice PA almeno una casella di posta elettronica certificata per ciascun registro di protocollo. La pubbliche***

amministrazioni utilizzano per le comunicazioni tra l'amministrazione ed i propri dipendenti la posta elettronica o altri strumenti informatici di comunicazione nel rispetto delle norme in materia di protezione dei dati personali e previa informativa agli interessati in merito al grado di riservatezza degli strumenti utilizzati.

48. *Posta elettronica certificata.*

1. ***La trasmissione telematica di comunicazioni che necessitano di una ricevuta di invio e di una ricevuta di consegna avviene mediante la posta elettronica certificata ai sensi del decreto del Presidente della Repubblica 11 febbraio 2005, n. 68, o mediante altre soluzioni tecnologiche individuate con decreto del Presidente del Consiglio dei Ministri, sentito DigitPA.***
2. ***La trasmissione del documento informatico per via telematica, effettuata ai sensi del comma 1, equivale, salvo che la legge disponga diversamente, alla notificazione per mezzo della posta.***
3. ***La data e l'ora di trasmissione e di ricezione di un documento informatico trasmesso ai sensi del comma 1 sono opponibili ai terzi se conformi alle disposizioni di cui al decreto del Presidente della Repubblica 11 febbraio 2005, n. 68, ed alle relative regole tecniche, ovvero conformi al decreto del Presidente del Consiglio dei Ministri di cui al comma 1.***

49. *Segretezza della corrispondenza trasmessa per via telematica.*

1. Gli addetti alle operazioni di trasmissione per via telematica di atti, dati e documenti formati con strumenti informatici non possono prendere cognizione della corrispondenza telematica, duplicare con qualsiasi mezzo o cedere a terzi a qualsiasi titolo informazioni anche in forma sintetica o per estratto sull'esistenza o sul contenuto di corrispondenza, comunicazioni o messaggi tra-

smessi per via telematica, salvo che si tratti di informazioni per loro natura o per espressa indicazione del mittente destinate ad essere rese pubbliche.

2. Agli effetti del presente codice, gli atti, i dati e i documenti trasmessi per via telematica si considerano, nei confronti del gestore del sistema di trasporto delle informazioni, di proprietà del mittente sino a che non sia avvenuta la consegna al destinatario.

Capo V - Dati delle pubbliche amministrazioni e servizi in rete

Sezione I - Dati delle pubbliche amministrazioni

50. *Disponibilità dei dati delle pubbliche amministrazioni.*

1. I dati delle pubbliche amministrazioni sono formati, raccolti, conservati, resi disponibili e accessibili con l'uso delle tecnologie dell'informazione e della comunicazione che ne consentano la fruizione e riutilizzazione, alle condizioni fissate dall'ordinamento, da parte delle altre pubbliche amministrazioni e dai privati; restano salvi i limiti alla conoscibilità dei dati previsti dalle leggi e dai regolamenti, le norme in materia di protezione dei dati personali ed il rispetto della normativa comunitaria in materia di riutilizzo delle informazioni del settore pubblico.
2. Qualunque dato trattato da una pubblica amministrazione, con le esclusioni di cui all'articolo 2, comma 6, salvi i casi previsti dall'articolo 24 della legge 7 agosto 1990, n. 241, e nel rispetto della normativa in materia di protezione dei dati personali, è reso accessibile e fruibile alle altre amministrazioni quando l'utilizzazione del dato sia necessaria per lo svolgimento dei compiti istituzionali dell'amministrazione richiedente, senza oneri a carico di quest'ultima, ***salvo per la prestazione di elaborazioni aggiuntive*** è fatto comunque salvo il disposto dell'articolo 43, comma 4, del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445.
3. Al fine di rendere possibile l'utilizzo in via telematica dei dati di una pubblica amministrazione da parte dei sistemi informatici di altre amministrazioni l'amministrazione titolare dei dati predispone, gestisce ed eroga i servizi informatici allo scopo necessari,

secondo le regole tecniche del sistema pubblico di connettività di cui al presente decreto.

Art. 50-bis. Continuità operativa.

1. ***In relazione ai nuovi scenari di rischio, alla crescente complessità dell'attività istituzionale caratterizzata da un intenso utilizzo della tecnologia dell'informazione, le pubbliche amministrazioni predispongono i piani di emergenza in grado di assicurare la continuità delle operazioni indispensabili per il servizio e il ritorno alla normale operatività.***
2. ***Il Ministro per la pubblica amministrazione e l'innovazione assicura l'omogeneità delle soluzioni di continuità operativa definite dalle diverse Amministrazioni e ne informa con cadenza almeno annuale il Parlamento.***
3. ***A tali fini, le pubbliche amministrazioni definiscono :***
   a) ***il piano di continuità operativa, che fissa gli obiettivi e i principi da perseguire, descrive le procedure per la gestione della continuità operativa, anche affidate a soggetti esterni. Il piano tiene conto delle potenziali criticità relative a risorse umane, strutturali, tecnologiche e contiene idonee misure preventive. Le amministrazioni pubbliche verificano la funzionalità del piano di continuità operativa con cadenza biennale;***
   b) ***il piano di disaster recovery, che costituisce parte integrante di quello di continuità operativa di cui alla lettera a) e stabilisce le misure tecniche e organizzative per garantire il funzionamento dei centri di elaborazione dati e delle procedure informatiche rilevanti in siti alternativi a quelli di produzione. DigitPA, sentito il Garante per la protezione dei dati personali, definisce le linee guida per le soluzioni tecniche idonee a garantire la salvaguardia dei dati e delle applicazioni informatiche, verifica annualmente il costante aggiornamento dei piani di disaster recovery delle amministrazioni interessate e ne informa annualmente il Ministro per la pubblica amministrazione e l'innovazione.***

4. I piani di cui al comma 3 sono adottati da ciascuna amministrazione sulla base di appositi e dettagliati studi di fattibilità tecnica; su tali studi è obbligatoriamente acquisito il parere di DigitPA.

51. (***Sicurezza dei dati, dei sistemi e delle infrastrutture delle pubbliche amministrazioni***).

1. Con le regole tecniche adottate ai sensi dell'articolo 71 sono individuate le modalità che garantiscono l'esattezza, la disponibilità, l'accessibilità, l'integrità e la riservatezza dei dati, dei sistemi e delle infrastrutture.

1-bis. DigitPA, ai fini dell'attuazione del comma 1:

a) raccorda le iniziative di prevenzione e gestione degli incidenti di sicurezza informatici;

b) promuove intese con le analoghe strutture internazionali;

c) segnala al Ministro per la pubblica amministrazione e l'innovazione il mancato rispetto delle regole tecniche di cui al comma 1 da parte delle pubbliche amministrazioni.";

d) dopo il comma 2, è aggiunto il seguente: "2-bis. Le amministrazioni hanno l'obbligo di aggiornare tempestivamente i dati nei propri archivi, non appena vengano a conoscenza dell'inesattezza degli stessi.".

2. I documenti informatici delle pubbliche amministrazioni devono essere custoditi e controllati con modalità tali da ridurre al minimo i rischi di distruzione, perdita, accesso non autorizzato o non consentito o non conforme alle finalità della raccolta.

2-bis. Le amministrazioni hanno l'obbligo di aggiornare tempestivamente i dati nei propri archivi, non appena vengano a conoscenza dell'inesattezza degli stessi.

52. ***Accesso telematico e riutilizzazione dei*** *dati e documenti delle pubbliche amministrazioni*

1. L'accesso telematico a dati, documenti e procedimenti è disciplinato dalle pubbliche amministrazioni secondo le disposizioni del presente codice e nel rispetto delle disposizioni di legge e di regolamento in materia di protezione dei dati personali, di accesso ai documenti amministrativi, di tutela del segreto e di divieto di divulgazione. I regolamenti che disciplinano l'esercizio del diritto di accesso sono pubblicati su siti pubblici accessibili per via telematica.

1-bis. Le pubbliche amministrazioni, al fine di valorizzare e rendere fruibili i dati pubblici di cui sono titolari, promuovono progetti di elaborazione e di diffusione degli stessi anche attraverso l'uso di strumenti di finanza di progetto, assicurando:

a) il rispetto di quanto previsto dall'articolo 54, comma 3;

b) la pubblicazione dei dati e dei documenti in formati aperti di cui all'articolo 68, commi 3 e 4.

53. *Caratteristiche dei siti.*

1. Le pubbliche amministrazioni centrali realizzano siti istituzionali su reti telematiche che rispettano i princìpi di accessibilità, nonché di elevata usabilità e reperibilità, anche da parte delle persone disabili, completezza di informazione, chiarezza di linguaggio, affidabilità, semplicità dì consultazione, qualità, omogeneità ed interoperabilità. Sono in particolare resi facilmente reperibili e consultabili i dati di cui all'articolo 54.
2. Il CNIPA svolge funzioni consultive e di coordinamento sulla realizzazione e modificazione dei siti delle amministrazioni centrali.
3. Lo Stato promuove intese ed azioni comuni con le regioni e le autonomie locali affinché realizzino siti istituzionali con le caratteristiche di cui al comma 1.

54. *Contenuto dei siti delle pubbliche amministrazioni.*

1. I siti delle pubbliche amministrazioni contengono necessariamente i seguenti dati pubblici:
   a) l'organigramma, l'articolazione degli uffici, le attribuzioni e l'organizzazione di ciascun ufficio anche di livello dirigenziale non generale, i nomi dei dirigenti responsabili dei singoli uffici, nonché il settore dell'ordinamento giuridico riferibile all'attività da essi svolta, corredati dai documenti anche normativi di riferimento;
   b) l'elenco delle tipologie di procedimento svolte da ciascun ufficio di livello dirigenziale non generale, il termine per la conclusione di ciascun procedimento ed ogni altro termine procedimentale, il nome del responsabile e l'unità organizzativa responsabile dell'istruttoria e di ogni altro adempimento procedimentale, nonché dell'adozione del provvedimento finale, come individuati ai sensi degli articoli 2, 4 e 5 della legge 7 agosto 1990, n. 241;
   c) le scadenze e le modalità di adempimento dei procedimenti individuati ai sensi degli articoli 2 e 4 della legge 7 agosto 1990, n. 241;
   d) l'elenco completo delle caselle di posta elettronica istituzionali attive, specificando anche se si tratta di una casella di posta elettronica certificata di cui al decreto del Presidente della Repubblica 11 febbraio 2005, n. 68;
   e) le pubblicazioni di cui all'articolo 26 della legge 7 agosto 1990, n. 241, nonché i messaggi di informazione e di comunicazione previsti dalla legge 7 giugno 2000, n. 150;
   f) l'elenco di tutti i bandi di gara;
   g) l'elenco dei servizi forniti in rete già disponibili e dei servizi di futura attivazione, indicando i tempi previsti per l'attivazione medesima.
   g-bis) i bandi di concorso.

1-bis. Le pubbliche amministrazioni centrali comunicano in via telematica alla Presidenza del Consiglio dei Ministri – Dipartimento della funzione pubblica i dati di cui alle lettere b), c) , g) e g-bis) del comma 1, secondo i criteri e le modalità di trasmissione e aggiornamento individuati con circolare del Ministro per la pubblica amministrazione e

l'innovazione. I dati di cui al periodo precedente sono pubblicati sul sito istituzionale del Dipartimento della funzione pubblica. La mancata comunicazione o aggiornamento dei dati è comunque rilevante ai fini della misurazione e valutazione della performance individuale dei dirigenti.

2 Abrogato

2-bis Abrogato

2-ter. Le amministrazioni pubbliche pubblicano nei propri siti un indirizzo istituzionale di posta elettronica certificata a cui il cittadino possa rivolgersi per qualsiasi richiesta ai sensi del presente codice. Le amministrazioni devono altresì assicurare un servizio che renda noti al pubblico i tempi di risposta.

2-*quater*. Le amministrazioni pubbliche che già dispongono di propri siti devono pubblicare il registro dei processi automatizzati rivolti al pubblico. Tali processi devono essere dotati di appositi strumenti per la verifica a distanza da parte del cittadino dell'avanzamento delle pratiche ***che lo riguardano.***

3. I dati pubblici contenuti nei siti delle pubbliche amministrazioni sono fruibili in rete gratuitamente e senza necessità di ***identificazione*** informatica.
4. Le pubbliche amministrazioni garantiscono che le informazioni contenute sui siti siano conformi e corrispondenti alle informazioni contenute nei provvedimenti amministrativi originali dei quali si fornisce comunicazione tramite il sito.

4-*bis*. La pubblicazione telematica produce effetti di pubblicità legale nei casi e nei modi espressamente previsti dall'ordinamento.

55. *Consultazione delle iniziative normative del Governo*.

1. La Presidenza del Consiglio dei Ministri può pubblicare su sito telematico le notizie relative ad iniziative normative del Governo, nonché i disegni di legge di particolare rilevanza, assicurando forme di partecipazione del cittadino in conformità con le disposizioni vigenti in materia di tutela delle persone e di altri soggetti rispetto al trattamento di dati personali. La Presidenza del Consi-

glio dei Ministri può inoltre pubblicare atti legislativi e regolamentari in vigore, nonché i massimari elaborati da organi di giurisdizione.

2. Con decreto del Presidente del Consiglio dei Ministri sono individuate le modalità di partecipazione del cittadino alla consultazione gratuita in via telematica.

56. *Dati identificativi delle questioni pendenti dinanzi all'autorità giudiziaria di ogni ordine e grado.*

1. I dati identificativi delle questioni pendenti dinanzi al giudice amministrativo e contabile sono resi accessibili a chi vi abbia interesse mediante pubblicazione sul sistema informativo interno e sul sito istituzionale delle autorità emananti.
2. Le sentenze e le altre decisioni del giudice amministrativo e contabile, rese pubbliche mediante deposito in segreteria, sono contestualmente inserite nel sistema informativo interno e sul sito istituzionale, osservando le cautele previste dalla normativa in materia di tutela dei dati personali.

2-bis. I dati identificativi delle questioni pendenti, le sentenze e le altre decisioni depositate in cancelleria o segreteria dell'autorità giudiziaria di ogni ordine e grado sono, comunque, rese accessibili ai sensi dell'articolo 51 del codice in materia di protezione dei dati personali approvato con decreto legislativo n. 196 del 2003.

57. *Moduli e formulari.*

1. Le pubbliche amministrazioni provvedono a definire e a ***rendere disponibili per via telematica*** l'elenco della documentazione richiesta per i singoli procedimenti, i moduli e i formulari validi ad ogni effetto di legge, anche ai fini delle dichiarazioni sostitutive di certificazione e delle dichiarazioni sostitutive di notorietà.
2. ***Le pubbliche amministrazioni non possono richiedere l'uso di moduli e formulari che non siano stati pubblicati; in caso di omessa pubblicazione, i relativi procedimenti possono***

***essere avviati anche in assenza dei suddetti moduli o formulari. La mancata pubblicazione è altresì rilevante ai fini della misurazione e valutazione della performance individuale dei dirigenti responsabili.*.**

57-bis. *Indice degli indirizzi delle pubbliche amministrazioni.*

1. Al fine di assicurare la trasparenza delle attività istituzionali è istituito l'indice degli indirizzi delle amministrazioni pubbliche, nel quale sono indicati gli indirizzi di posta elettronica da utilizzare per le comunicazioni e per lo scambio di informazioni e per l'invio di documenti a tutti gli effetti di legge fra le amministrazioni e fra le amministrazioni ed i cittadini.
2. ***La realizzazione e la gestione dell'indice sono affidate a DigitPA, che può utilizzare a tal fine elenchi e repertori già formati dalle amministrazioni pubbliche.***
3. Le amministrazioni aggiornano gli indirizzi ed i contenuti dell'indice con cadenza almeno semestrale, salvo diversa indicazione del CNIPA. La mancata comunicazione degli elementi necessari al completamento dell'indice e del loro aggiornamento è valutata ai fini della responsabilità dirigenziale e dell'attribuzione della retribuzione di risultato ai dirigenti responsabili.

Sezione II - Fruibilità dei dati

58. *Modalità della fruibilità del dato.*

1. Il trasferimento di un dato da un sistema informativo ad un altro non modifica la titolarità del dato.
2. ***Ai sensi dell'articolo 50, comma 2, nonché al fine di agevolare l'acquisizione d'ufficio ed il controllo sulle dichiarazioni sostitutive riguardanti informazioni e dati relativi a stati, qualità personali e fatti di cui agli articoli 46 e 47 del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, le Amministrazioni titolari di banche dati accessibili per via telematica predispongono, sulla base delle linee***

guida redatte da DigitPA, sentito il Garante per la protezione dei dati personali, apposite convenzioni aperte all'adesione di tutte le amministrazioni interessate volte a disciplinare le modalità di accesso ai dati da parte delle stesse amministrazioni procedenti, senza oneri a loro carico. Le convenzioni valgono anche quale autorizzazione ai sensi dell'articolo 43, comma 2, del citato decreto del Presidente della Repubblica n. 445 del 2000.

3. ***DigitPA provvede al monitoraggio dell'attuazione del presente articolo, riferendo annualmente con apposita relazione al Ministro per la pubblica amministrazione e l'innovazione e alla Commissione per la valutazione, la trasparenza e l'integrità delle amministrazione pubbliche di cui all'articolo 13 del decreto legislativo 27 ottobre 2009, n. 150.***

3-bis. In caso di mancata predisposizione delle convenzioni di cui al comma 2, il Presidente del Consiglio dei Ministri stabilisce un termine entro il quale le amministrazioni interessate devono provvedere. Decorso inutilmente il termine, il Presidente del Consiglio dei Ministri può nominare un commissario ad acta incaricato di predisporre le predette convenzioni. Al Commissario non spettano compensi, indennità o rimborsi.

3-ter. Resta ferma la speciale disciplina dettata in materia di dati territoriali.

59. *Dati territoriali.*

1. Per dato territoriale si intende qualunque informazione geograficamente localizzata.
2. È istituito il Comitato per le regole tecniche sui dati territoriali delle pubbliche amministrazioni, con il compito di definire le regole tecniche per la realizzazione delle basi dei dati territoriali, la documentazione, la fruibilità e lo scambio dei dati stessi tra le pubbliche amministrazioni centrali e locali in coerenza con le di-

sposizioni del presente decreto che disciplinano il sistema pubblico di connettività.

3. Per agevolare la pubblicità dei dati di interesse generale, disponibili presso le pubbliche amministrazioni a livello nazionale, regionale e locale, presso il CNIPA è istituito il Repertorio nazionale dei dati territoriali.
4. Ai sensi dell'articolo 17, comma 3, della legge 23 agosto 1988, n. 400, con uno o più decreti sulla proposta del Presidente del Consiglio dei Ministri o, per sua delega, del Ministro per l'innovazione e le tecnologie, previa intesa con la Conferenza unificata di cui all'articolo 8 decreto legislativo 28 agosto 1997, n. 281, sono definite la composizione e le modalità per il funzionamento del Comitato di cui al comma 2.
5. ***Con decreti del Presidente del Consiglio dei Ministri o del Ministro delegato per la pubblica amministrazione e l'innovazione,*** di concerto con il Ministro dell'ambiente e della tutela del territorio e del mare, per i profili relativi ai dati ambientali, sentito il Comitato per le regole tecniche sui dati territoriali delle pubbliche amministrazioni, e sentita la Conferenza unificata di cui all'articolo 8 del decreto legislativo 28 luglio 1998, n. 281, sono definite le regole tecniche per la definizione del contenuto del repertorio nazionale dei dati territoriali, nonché delle modalità di prima costituzione e di successivo aggiornamento dello stesso, per la formazione, la documentazione e lo scambio dei dati territoriali detenuti dalle singole amministrazioni competenti, nonché le regole ed i costi per l'utilizzo dei dati stessi tra le pubbliche amministrazioni centrali e locali e da parte dei privati.
6. La partecipazione al Comitato non comporta oneri né alcun tipo di spese ivi compresi compensi o gettoni di presenza. Gli eventuali rimborsi per spese di viaggio sono a carico delle amministrazioni direttamente interessate che vi provvedono nell'àmbito degli ordinari stanziamenti di bilancio.
7. Agli oneri finanziari di cui al comma 3 si provvede con il fondo di finanziamento per i progetti strategici del settore informatico di cui all'articolo 27, comma 2, della legge 16 gennaio 2003, n. 3.

7-bis. Nell'ambito dei dati territoriali di interesse nazionale rientra la base dei dati catastali gestita dall'Agenzia del territorio. Per garantire la circolazione e la fruizione dei dati catastali conformemente

alle finalità ed alle condizioni stabilite dall'articolo 50, il direttore dell'Agenzia del territorio, di concerto con il Comitato per le regole tecniche sui dati territoriali delle pubbliche amministrazioni e previa intesa con la Conferenza unificata, definisce con proprio decreto entro la data del 30 giugno 2006, in coerenza con le disposizioni che disciplinano il sistema pubblico di connettività, le regole tecnico economiche per l'utilizzo dei dati catastali per via telematica da parte dei sistemi informatici di altre amministrazioni.

60. *Base di dati di interesse nazionale.*

1. Si definisce base di dati di interesse nazionale l'insieme delle informazioni raccolte e gestite digitalmente dalle pubbliche amministrazioni, omogenee per tipologia e contenuto e la cui conoscenza è utilizzabile dalle pubbliche amministrazioni***, anche per fini statistici,*** per l'esercizio delle proprie funzioni e nel rispetto delle competenze e delle normative vigenti.
2. Ferme le competenze di ciascuna pubblica amministrazione, le basi di dati di interesse nazionale costituiscono, per ciascuna tipologia di dati, un sistema informativo unitario che tiene conto dei diversi livelli istituzionali e territoriali e che garantisce l'allineamento delle informazioni e l'accesso alle medesime da parte delle pubbliche amministrazioni interessate. La realizzazione di tali sistemi informativi e le modalità di aggiornamento sono attuate secondo le regole tecniche sul sistema pubblico di connettività ***di cui all'articolo 73 e secondo le vigenti regole del Sistema statistico nazionale di cui al decreto legislativo 6 settembre 1989, n. 322, e successive modificazioni***.
3. Le basi di dati di interesse nazionale sono individuate con decreto del Presidente del Consiglio dei Ministri, su proposta del Presidente del Consiglio dei Ministri o del Ministro delegato per l'innovazione e le tecnologie, di concerto con i Ministri di volta in volta interessati, d'intesa con la Conferenza unificata di cui all'articolo 8 del decreto legislativo 28 agosto 1997, n. 281, nelle materie di competenza e ***sentiti il Garante per la protezione dei dati personali e l'Istituto nazionale di statistica.*** Con il medesimo decreto sono altresì individuate le strutture responsa-

bili della gestione operativa di ciascuna base di dati e le caratteristiche tecniche del sistema informativo di cui al comma 2.

3-bis. In sede di prima applicazione e fino all'adozione del decreto di cui al comma 3, sono individuate le seguenti basi di dati di interesse nazionale:

- **a)** ***repertorio nazionale dei dati territoriali;***
- **b)** ***indice nazionale delle anagrafi;***
- **c)** ***banca dati nazionale dei contratti pubblici di cui all'articolo 62-bis;***
- **d)** ***casellario giudiziale;***
- **e)** ***registro delle imprese;***
- **f)** ***gli archivi automatizzati in materia di immigrazione e di asilo di cui all'articolo 2, comma 2, del decreto del Presidente della Repubblica 27 luglio 2004, n. 242.***

4. Agli oneri finanziari di cui al presente articolo si provvede con il fondo di finanziamento per i progetti strategici del settore informatico di cui all'articolo 27, comma 2, della legge 16 gennaio 2003, n. 3.

61. *Delocalizzazione dei registri informatici.*

1. Fermo restando il termine di cui all'articolo 40, comma 4, i pubblici registri immobiliari possono essere formati e conservati su supporti informatici in conformità alle disposizioni del presente codice, secondo le regole tecniche stabilite dall'articolo 71, nel rispetto della normativa speciale e dei princìpi stabiliti dal codice civile. In tal caso i predetti registri possono essere conservati anche in luogo diverso dall'Ufficio territoriale competente.

62. *Indice nazionale delle anagrafi.*

1. L'Indice nazionale delle anagrafi (INA), di cui all'articolo 1 della legge 24 dicembre 1954, n. 1228, è realizzato con strumenti informatici e nel rispetto delle regole tecniche concernenti il sistema pubblico di connettività, in coerenza con le quali il Ministero

dell'interno definisce le regole di sicurezza per l'accesso e per la gestione delle informazioni anagrafiche e fornisce i servizi di convalida delle informazioni medesime ove richiesto per l'attuazione della normativa vigente.

62-bis. *Banca dati nazionale dei contratti pubblici.*

1. **Per favorire la riduzione degli oneri amministrativi derivanti dagli obblighi informativi ed assicurare l'efficacia, la trasparenza e il controllo in tempo reale dell'azione amministrativa per l'allocazione della spesa pubblica in lavori, servizi e forniture, anche al fine del rispetto della legalità e del corretto agire della pubblica amministrazione e prevenire fenomeni di corruzione, si utilizza la "Banca dati nazionale dei contratti pubblici" (BDNCP) istituita, presso l'Autorità per la vigilanza sui contratti pubblici di lavori, servizi e forniture, della quale fanno parte i dati previsti dall'articolo 7 del decreto legislativo 12 aprile 2006, n. 163, e disciplinata, ai sensi del medesimo decreto legislativo, dal relativo regolamento attuativo.**

Sezione III - Servizi in rete

63. *Organizzazione e finalità dei servizi in rete.*

1. Le pubbliche amministrazioni centrali individuano le modalità di erogazione dei servizi in rete in base a criteri di valutazione di efficacia, economicità ed utilità e nel rispetto dei princìpi di eguaglianza e non discriminazione, tenendo comunque presenti le dimensioni dell'utenza, la frequenza dell'uso e l'eventuale destinazione all'utilizzazione da parte di categorie in situazioni di disagio.
2. ***Le pubbliche amministrazioni e i gestori di servizi pubblici progettano e realizzano i servizi in rete mirando alla migliore soddisfazione delle esigenze degli utenti, in particolare garantendo la completezza del procedimento, la certifica-***

zione dell'esito e l'accertamento del grado di soddisfazione dell'utente, A tal fine, sono tenuti ad adottare strumenti idonei alla rilevazione immediata, continua e sicura del giudizio degli utenti, in conformità alle regole tecniche da emanare ai sensi dell'articolo 71. Per le amministrazioni e i gestori di servizi pubblici regionali e locali le regole tecniche sono adottate previo parere della Commissione permanente per l'innovazione tecnologica nelle regioni e negli enti locali di cui all'articolo 14, comma 3-bis.

3. Le pubbliche amministrazioni collaborano per integrare i procedimenti di rispettiva competenza al fine di agevolare gli adempimenti di cittadini ed imprese e rendere più efficienti i procedimenti che interessano più amministrazioni, attraverso idonei sistemi di cooperazione.

64. *Modalità di accesso ai servizi erogati in rete dalle pubbliche amministrazioni.*

1. La carta d'identità elettronica e la carta nazionale dei servizi costituiscono strumenti per l'accesso ai servizi erogati in rete dalle pubbliche amministrazioni per i quali sia necessaria l'***identificazione*** informatica.
2. ***Le pubbliche amministrazioni possono consentire l'accesso ai servizi in rete da esse erogati che richiedono l'identificazione informatica anche con strumenti diversi dalla carta d'identità elettronica e dalla carta nazionale dei servizi, purché tali strumenti consentano l'individuazione del soggetto che richiede il servizio.*** L'accesso con carta d'identità elettronica e carta nazionale dei servizi è comunque consentito indipendentemente dalle modalità di accesso predisposte dalle singole amministrazioni.
3. ***Abrogato***

65. *Istanze e dichiarazioni presentate alle pubbliche amministrazioni per via telematica.*

1. Le istanze e le dichiarazioni presentate alle pubbliche amministrazioni per via telematica ai sensi dell'articolo 38, commi 1 e 3, del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, sono valide:
   a) se sottoscritte mediante la firma digitale, il cui certificato è rilasciato da un certificatore accreditato;
   b) ovvero, quando l'autore è identificato dal sistema informatico con l'uso della carta d'identità elettronica o della carta nazionale dei servizi, nei limiti di quanto stabilito da ciascuna amministrazione ai sensi della normativa vigente;
   c) ovvero quando l'autore è identificato dal sistema informatico con i diversi strumenti di cui all'articolo 64, comma 2, nei limiti di quanto stabilito da ciascuna amministrazione ai sensi della normativa vigente, ***nonché quando le istanze e le dichiarazioni sono inviate con le modalità di cui all'articolo 38, comma 3, del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445.***
   c-bis) ovvero se trasmesse dall'autore mediante la propria casella di posta elettronica certificata purché le relative credenziali di accesso siano state rilasciate previa identificazione del titolare, anche per via telematica secondo modalità definite con regole tecniche adottate ai sensi dell'articolo 71, e ciò sia attestato dal gestore del sistema nel messaggio o in un suo allegato. In tal caso, la trasmissione costituisce dichiarazione vincolante ai sensi dell'articolo 6, comma 1, secondo periodo. Sono fatte salve le disposizioni normative che prevedono l'uso di specifici sistemi di trasmissione telematica nel settore tributario.

1-bis. Con decreto del Ministro per la pubblica amministrazione e l'innovazione e del Ministro per la semplificazione normativa, su proposta dei Ministri competenti per materia, possono essere individuati i casi in cui è richiesta la sottoscrizione mediante firma digitale.

2. Le istanze e le dichiarazioni inviate o compilate sul sito secondo le modalità previste dal comma 1 sono equivalenti alle istanze e alle dichiarazioni sottoscritte con firma autografa apposta in presenza del dipendente addetto al procedimento.
3. **Abrogato**

4. Il comma 2 dell'articolo 38 del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, è sostituito dal seguente:
   «2. Le istanze e le dichiarazioni inviate per via telematica sono valide se effettuate secondo quanto previsto dall'articolo 65 del decreto legislativo 7 marzo 2005, n. 82.

Sezione IV - Carte elettroniche

66. *Carta d'identità elettronica e carta nazionale dei servizi.*

1. Le caratteristiche e le modalità per il rilascio della carta d'identità elettronica e dell'analogo documento, rilasciato a seguito della denuncia di nascita e prima del compimento ***dell'età prevista dalla legge per il rilascio della carta d'identità elettronica***, sono definite con decreto del Presidente del Consiglio dei Ministri, adottato su proposta del Ministro dell'interno, di concerto con il Ministro per la funzione pubblica, con il Ministro per l'innovazione e le tecnologie e con il Ministro dell'economia e delle finanze, sentito il Garante per la protezione dei dati personali e d'intesa con la Conferenza unificata di cui all'articolo 8 del decreto legislativo 28 agosto 1997, n. 281.
2. Le caratteristiche e le modalità per il rilascio, per la diffusione e l'uso della carta nazionale dei servizi sono definite con uno o più regolamenti, ai sensi dell'articolo 17, comma 2, della legge 23 agosto 1988, n. 400, adottati su proposta congiunta dei Ministri per la funzione pubblica e per l'innovazione e le tecnologie, di concerto con il Ministro dell'economia e delle finanze, sentito il Garante per la protezione dei dati personali e d'intesa con la Conferenza unificata di cui all'articolo 8 del decreto legislativo 28 agosto 1997, n. 281, nel rispetto dei seguenti princìpi:
   a) all'emissione della carta nazionale dei servizi provvedono, su richiesta del soggetto interessato, le pubbliche amministrazioni che intendono rilasciarla;
   b) l'onere economico di produzione e rilascio della carta nazionale dei servizi è a carico delle singole amministrazioni che le emettono;

c) eventuali indicazioni di carattere individuale connesse all'erogazione dei servizi al cittadino, sono possibili nei limiti di cui al decreto legislativo 30 giugno 2003, n. 196;
d) le pubbliche amministrazioni che erogano servizi in rete devono consentirne l'accesso ai titolari della carta nazionale dei servizi indipendentemente dall'ente di emissione, che è responsabile del suo rilascio;
e) la carta nazionale dei servizi può essere utilizzata anche per i pagamenti informatici tra soggetti privati e pubbliche amministrazioni, secondo quanto previsto dalla normativa vigente.

3. La carta d'identità elettronica e l'analogo documento, rilasciato a seguito della denuncia di nascita e prima del compimento ***dell'età prevista dalla legge per il rilascio della carta d'identità elettronica***, devono contenere:
   a) i dati identificativi della persona;
   b) il codice fiscale.
4. La carta d'identità elettronica e l'analogo documento, rilasciato a seguito della denuncia di nascita e prima del compimento ***dell'età prevista dalla legge per il rilascio della carta d'identità elettronica***, possono contenere, a richiesta dell'interessato ove si tratti di dati sensibili:
   a) l'indicazione del gruppo sanguigno;
   b) le opzioni di carattere sanitario previste dalla legge;
   c) i dati biometrici indicati col decreto di cui al comma 1, con esclusione, in ogni caso, del DNA;
   d) tutti gli altri dati utili al fine di razionalizzare e semplificare l'azione amministrativa e i servizi resi al cittadino, anche per mezzo dei portali, nel rispetto della normativa in materia di riservatezza;
   e) le procedure informatiche e le informazioni che possono o debbono essere conosciute dalla pubblica amministrazione e da altri soggetti, occorrenti per la firma elettronica.
5. La carta d'identità elettronica e la carta nazionale dei servizi possono essere utilizzate quali strumenti di autenticazione telematica per l'effettuazione di pagamenti tra soggetti privati e pubbliche amministrazioni, secondo le modalità stabilite con le regole tecniche di cui all'articolo 71, di concerto con il Ministro dell'economia e delle finanze, sentita la Banca d'Italia.

6. Con decreto del Ministro dell'interno, del Ministro per l'innovazione e le tecnologie e del Ministro dell'economia e delle finanze, sentito il Garante per la protezione dei dati personali e d'intesa con la Conferenza unificata di cui all'articolo 8 del decreto legislativo 28 agosto 1997, n. 281, sono dettate le regole tecniche e di sicurezza relative alle tecnologie e ai materiali utilizzati per la produzione della carta di identità elettronica, del documento di identità elettronico e della carta nazionale dei servizi, nonché le modalità di impiego.
7. Nel rispetto della disciplina generale fissata dai decreti di cui al presente articolo e delle vigenti disposizioni in materia di protezione dei dati personali, le pubbliche amministrazioni, nell'àmbito dei rispettivi ordinamenti, possono sperimentare modalità di utilizzazione dei documenti di cui al presente articolo per l'erogazione di ulteriori servizi o utilità.
8. Le tessere di riconoscimento rilasciate dalle amministrazioni dello Stato ai sensi del decreto del Presidente della Repubblica 28 luglio 1967, n. 851, possono essere realizzate anche con modalità elettroniche e contenere le funzionalità della carta nazionale dei servizi per consentire l'accesso per via telematica ai servizi erogati in rete dalle pubbliche amministrazioni.

8-bis. Fino al 31 dicembre 2011, la carta nazionale dei servizi e le altre carte elettroniche ad essa conformi possono essere rilasciate anche ai titolari di carta di identità elettronica

Capo VI - Sviluppo, acquisizione e riuso di sistemi informatici nelle pubbliche amministrazioni

67. *Modalità di sviluppo ed acquisizione.*

1. Le pubbliche amministrazioni centrali, per i progetti finalizzati ad appalti di lavori e servizi ad alto contenuto di innovazione tecnologica, possono selezionare uno o più proposte utilizzando il concorso di idee di cui all'articolo 57 del decreto del Presidente della Repubblica 21 dicembre 1999, n. 554.
2. Le amministrazioni appaltanti possono porre a base delle gare aventi ad oggetto la progettazione, o l'esecuzione, o entrambe,

degli appalti di cui al comma 1, le proposte ideative acquisite ai sensi del comma 1, previo parere tecnico di congruità del CNIPA; alla relativa procedura è ammesso a partecipare, ai sensi dell'articolo 57, comma 6, del decreto del Presidente della Repubblica 21 dicembre 1999, n. 554, anche il soggetto selezionato ai sensi del comma 1, qualora sia in possesso dei relativi requisiti soggettivi.

68. *Analisi comparativa delle soluzioni.*

1. Le pubbliche amministrazioni, nel rispetto della legge 7 agosto 1990, n. 241, e del decreto legislativo 12 febbraio 1993, n. 39, acquisiscono, secondo le procedure previste dall'ordinamento, programmi informatici***, o parti di essi,*** a seguito di una valutazione comparativa di tipo tecnico ed economico tra le seguenti soluzioni disponibili sul mercato:
   a) sviluppo di programmi informatici per conto e a spese dell'amministrazione sulla scorta dei requisiti indicati dalla stessa amministrazione committente;
   b) riuso di programmi informatici sviluppati per conto e a spese della medesima o di altre amministrazioni;
   c) acquisizione di programmi informatici di tipo proprietario mediante ricorso a licenza d'uso;
   d) acquisizione di programmi informatici a codice sorgente aperto;
   e) acquisizione mediante combinazione delle modalità di cui alle lettere da a) a d).
2. ***Le pubbliche amministrazioni nella predisposizione o nell'acquisizione dei programmi informatici, adottano soluzioni informatiche, quando possibile modulari, basate sui sistemi funzionali resi noti ai sensi dell'articolo 70, che assicurino l'interoperabilità e la cooperazione applicativa e consentano la rappresentazione dei dati e documenti in più formati, di cui almeno uno di tipo aperto, salvo che ricorrano motivate ed eccezionali esigenze.***

2-***bis. Le amministrazioni pubbliche comunicano tempestivamente al DigitPA l'adozione delle applicazioni informatiche e delle pratiche tecnologiche, e organizzative,adottate,***

fornendo ogni utile informazione ai fini della piena conoscibilità delle soluzioni adottate e dei risultati ottenuti, anche per favorire il riuso e la più ampia diffusione delle migliori pratiche.

3. Per formato dei dati di tipo aperto si intende un formato dati reso pubblico e documentato esaustivamente.
4. Il CNIPA istruisce ed aggiorna, con periodicità almeno annuale, un repertorio dei formati aperti utilizzabili nelle pubbliche amministrazioni e delle modalità di trasferimento dei formati.

69. *Riuso dei programmi informatici.*

1. Le pubbliche amministrazioni che siano titolari di programmi ***informatici*** realizzati su specifiche indicazioni del committente pubblico, hanno obbligo di darli in formato sorgente, completi della documentazione disponibile, in uso gratuito ad altre pubbliche amministrazioni che li richiedono e che intendano adattarli alle proprie esigenze, salvo motivate ragioni.
2. Al fine di favorire il riuso dei programmi informatici di proprietà delle pubbliche amministrazioni, ai sensi del comma 1, nei capitolati o nelle specifiche di progetto è previsto ove possibile, che i programmi appositamente sviluppati per conto e a spese dell'amministrazione siano facilmente portabili su altre piattaforme ***e conformi alla definizione e regolamentazione effettuata da DigitPA, ai sensi dell'articolo 68, comma 2.***
3. Le pubbliche amministrazioni inseriscono, nei contratti per l'acquisizione di programmi informatici ***o di singoli moduli***, di cui al comma 1, clausole che garantiscano il diritto di disporre dei programmi ai fini del riuso da parte della medesima o di altre amministrazioni.
4. Nei contratti di acquisizione di programmi informatici sviluppati per conto e a spese delle amministrazioni, le stesse possono includere clausole, concordate con il fornitore, che tengano conto delle caratteristiche economiche ed organizzative di quest'ultimo, volte a vincolarlo, per un determinato lasso di tempo, a fornire, su richiesta di altre amministrazioni, servizi che consentono il ***riuso dei programmi o dei singoli moduli.*** Le clausole suddette

definiscono le condizioni da osservare per la prestazione dei servizi indicati.

70. *Banca dati dei programmi informatici riutilizzabili.*

1. ***DigitPA, sentita la Conferenza unificata di cui all'articolo 8 del decreto legislativo 28 agosto 1997, n. 281, valuta e rende note applicazioni tecnologiche realizzate dalle pubbliche amministrazioni, idonee al riuso da parte di altre pubbliche amministrazioni anche con riferimento a singoli moduli,segnalando quelle che, in base alla propria valutazione, si configurano quali migliori pratiche organizzative e tecnologiche.***
2. Le pubbliche amministrazioni centrali che intendono acquisire programmi applicativi valutano preventivamente la possibilità di riuso delle applicazioni analoghe rese note dal CNIPA ai sensi del comma 1, motivandone l'eventuale mancata adozione.

Capo VII - Regole tecniche

71. *Regole tecniche.*

1. ***Le regole tecniche previste nel presente codice sono dettate, con decreti del Presidente del Consiglio dei Ministri o del Ministro delegato per la pubblica amministrazione e l'innovazione, di concerto con i Ministri competenti, sentita la Conferenza unificata di cui all'articolo 8 del decreto legislativo 28 agosto 1997, n. 281, ed il Garante per la protezione dei dati personali nelle materie di competenza, previa acquisizione obbligatoria del parere tecnico di DigitPA.***

1-bis. Abrogato

1-ter. Le regole tecniche di cui al presente codice sono dettate in conformità alle discipline risultanti dal processo di standardizzazione tecnologica a livello internazionale ed alle normative dell'Unione europea.

2. Le regole tecniche vigenti nelle materie del presente codice restano in vigore fino all'adozione delle regole tecniche adottate ai sensi del presente articolo.

Capo VIII - Sistema pubblico di connettività e rete internazionale della pubblica amministrazione.

Sezione I - Definizioni relative al sistema pubblico di connettività

72. *Definizioni relative al sistema pubblico di connettività.*

1. Ai fini del presente decreto si intende per:
   a) «trasporto di dati»: i servizi per la realizzazione, gestione ed evoluzione di reti informatiche per la trasmissione di dati, oggetti multimediali e fonia;
   b) «interoperabilità di base»: i servizi per la realizzazione, gestione ed evoluzione di strumenti per lo scambio di documenti informatici fra le pubbliche amministrazioni e tra queste e i cittadini;
   c) «connettività»: l'insieme dei servizi di trasporto di dati e di interoperabilità di base;
   d) «interoperabilità evoluta»: i servizi idonei a favorire la circolazione, lo scambio di dati e informazioni, e l'erogazione fra le pubbliche amministrazioni e tra queste e i cittadini;
   e) «cooperazione applicativa»: la parte del sistema pubblico di connettività finalizzata all'interazione tra i sistemi informatici delle pubbliche amministrazioni per garantire l'integrazione dei metadati, delle informazioni e dei procedimenti amministrativi.

73. *Sistema pubblico di connettività (SPC).*

1. Nel rispetto dell'articolo 117, secondo comma, lettera r), della Costituzione, e nel rispetto dell'autonomia dell'organizzazione interna delle funzioni informative delle regioni e delle autonomie locali il presente Capo definisce e disciplina il Sistema pubblico di connettività (SPC), al fine di assicurare il coordinamento in-

formativo e informatico dei dati tra le amministrazioni centrali, regionali e locali e promuovere l'omogeneità nella elaborazione e trasmissione dei dati stessi, finalizzata allo scambio e diffusione delle informazioni tra le pubbliche amministrazioni e alla realizzazione di servizi integrati.

2. Il SPC è l'insieme di infrastrutture tecnologiche e di regole tecniche, per lo sviluppo, la condivisione, l'integrazione e la diffusione del patrimonio informativo e dei dati della pubblica amministrazione, necessarie per assicurare l'interoperabilità di base ed evoluta e la cooperazione applicativa dei sistemi informatici e dei flussi informativi, garantendo la sicurezza, la riservatezza delle informazioni, nonché la salvaguardia e l'autonomia del patrimonio informativo di ciascuna pubblica amministrazione.
3. La realizzazione del SPC avviene nel rispetto dei seguenti principi:
   a) sviluppo architetturale ed organizzativo atto a garantire la natura federata, policentrica e non gerarchica del sistema;
   b) economicità nell'utilizzo dei servizi di rete, di interoperabilità e di supporto alla cooperazione applicativa;
   c) sviluppo del mercato e della concorrenza nel settore delle tecnologie dell'informazione e della comunicazione.

3-bis. Le regole tecniche del Sistema pubblico di connettività sono dettate ai sensi dell'articolo 71.

74. *Rete internazionale delle pubbliche amministrazioni.*

1. Il presente decreto definisce e disciplina la Rete internazionale delle pubbliche amministrazioni, interconnessa al SPC. La Rete costituisce l'infrastruttura di connettività che collega, nel rispetto della normativa vigente, le pubbliche amministrazioni con gli uffici italiani all'estero, garantendo adeguati livelli di sicurezza e qualità.

Sezione II - Sistema pubblico di connettività SPC

75. *Partecipazione al Sistema pubblico di connettività.*

1. Al SPC partecipano tutte le amministrazioni di cui all'articolo 2, comma 2.
2. Il comma 1 non si applica alle amministrazioni di cui al decreto legislativo 30 marzo 2001, n. 165, limitatamente all'esercizio delle sole funzioni di ordine e sicurezza pubblica, difesa nazionale, consultazioni elettorali.
3. Ai sensi dell'articolo 3 del decreto del Presidente della Repubblica 11 novembre 1994, n. 680, nonché dell'articolo 25 del decreto legislativo 30 giugno 2003, n. 196, è comunque garantita la connessione con il SPC dei sistemi informativi degli organismi competenti per l'esercizio delle funzioni di sicurezza e difesa nazionale, nel loro esclusivo interesse e secondo regole tecniche che assicurino riservatezza e sicurezza. È altresì garantita la possibilità di connessione al SPC delle autorità amministrative indipendenti.

3-bis. Il gestore di servizi pubblici e i soggetti che perseguono finalità di pubblico interesse possono usufruire della connessione al SPC e dei relativi servizi, adeguandosi alle vigenti regole tecniche, previa delibera della Commissione di cui all'articolo 79

76. *Scambio di documenti informatici nell'ambito del Sistema pubblico di connettività.*

1. Gli scambi di documenti informatici tra le pubbliche amministrazioni nell'ambito del SPC, realizzati attraverso la cooperazione applicativa e nel rispetto delle relative procedure e regole tecniche di sicurezza, costituiscono invio documentale valido ad ogni effetto di legge.

77. *Finalità del Sistema pubblico di connettività.*

1. Al SPC sono attribuite le seguenti finalità:

a) fornire un insieme di servizi di connettività condivisi dalle pubbliche amministrazioni interconnesse, definiti negli aspetti di funzionalità, qualità e sicurezza, ampiamente graduabili in modo da poter soddisfare le differenti esigenze delle pubbliche amministrazioni aderenti al SPC;
b) garantire l'interazione della pubblica amministrazione centrale e locale con tutti gli altri soggetti connessi a Internet, nonché con le reti di altri enti, promuovendo l'erogazione di servizi di qualità e la miglior fruibilità degli stessi da parte dei cittadini e delle imprese;
c) fornire un'infrastruttura condivisa di interscambio che consenta l'interoperabilità tra tutte le reti delle pubbliche amministrazioni esistenti, favorendone lo sviluppo omogeneo su tutto il territorio nella salvaguardia degli investimenti effettuati;
d) fornire servizi di connettività e cooperazione alle pubbliche amministrazioni che ne facciano richiesta, per permettere l'interconnessione delle proprie sedi e realizzare così anche l'infrastruttura interna di comunicazione;
e) realizzare un modello di fornitura dei servizi multifornitore coerente con l'attuale situazione di mercato e le dimensioni del progetto stesso;
f) garantire lo sviluppo dei sistemi informatici nell'ambito del SPC salvaguardando la sicurezza dei dati, la riservatezza delle informazioni, nel rispetto dell'autonomia del patrimonio informativo delle singole amministrazioni e delle vigenti disposizioni in materia di protezione dei dati personali.

78. *Compiti delle pubbliche amministrazioni nel Sistema pubblico di connettività.*

1. Le pubbliche amministrazioni nell'ambito della loro autonomia funzionale e gestionale adottano nella progettazione e gestione dei propri sistemi informativi, ivi inclusi gli aspetti organizzativi, soluzioni tecniche compatibili con la cooperazione applicativa con le altre pubbliche amministrazioni, secondo le regole tecniche di cui ***all'articolo 73, comma 3-bis***. **Le stesse pubbliche amministrazioni, ove venga loro attribuito, per norma, il**

compito di gestire soluzioni infrastrutturali per l'erogazione di servizi comuni a più amministrazioni, adottano le medesime regole per garantire la compatibilità con la cooperazione applicativa potendosi avvalere di modalità atte a mantenere distinti gli ambiti di competenza.

2. Per le amministrazioni di cui all'articolo 1, comma 1, del decreto legislativo 12 febbraio 1993, n. 39, le responsabilità di cui al comma 1 sono attribuite al dirigente responsabile dei sistemi informativi automatizzati, di cui all'articolo 10, comma 1, dello stesso decreto legislativo (83).

2-bis. Le pubbliche amministrazioni centrali e periferiche di cui all'articolo 1, comma 1, lettera z), del presente codice, inclusi gli istituti e le scuole di ogni ordine e grado, le istituzioni educative e le istituzioni universitarie, nei limiti di cui all'articolo 1, comma 449, secondo periodo, della legge 27 dicembre 2006, n. 296, sono tenute, a decorrere dal 1° gennaio 2008 e comunque a partire dalla scadenza dei contratti relativi ai servizi di fonia in corso alla data predetta ad utilizzare i servizi «Voce tramite protocollo Internet» (VoIP) previsti dal sistema pubblico di connettività o da analoghe convenzioni stipulate da CONSIP.

2-ter. Il CNIPA effettua azioni di monitoraggio e verifica del rispetto delle disposizioni di cui al comma 2-bis.

2-quater. Il mancato adeguamento alle disposizioni di cui al comma 2-bis comporta la riduzione, nell'esercizio finanziario successivo, del 30 per cento delle risorse stanziate nell'anno in corso per spese di telefonia.

79. *Commissione di coordinamento del Sistema pubblico di connettività.*

1. È istituita la Commissione di coordinamento del SPC, di seguito denominata: «Commissione», preposta agli indirizzi strategici del SPC.
2. La Commissione:
   a) assicura il raccordo tra le amministrazioni pubbliche, nel rispetto delle funzioni e dei compiti spettanti a ciascuna di esse;

b) approva le linee guida, le modalità operative e di funzionamento dei servizi e delle procedure per realizzare la cooperazione applicativa fra i servizi erogati dalle amministrazioni;
c) promuove l'evoluzione del modello organizzativo e dell'architettura tecnologica del SPC in funzione del mutamento delle esigenze delle pubbliche amministrazioni e delle opportunità derivanti dalla evoluzione delle tecnologie;
d) promuove la cooperazione applicativa fra le pubbliche amministrazioni, nel rispetto delle regole tecniche di cui all'articolo 71;
e) definisce i criteri e ne verifica l'applicazione in merito alla iscrizione, sospensione e cancellazione dagli elenchi dei fornitori qualificati SPC di cui all'articolo 82;
f) dispone la sospensione e cancellazione dagli elenchi dei fornitori qualificati di cui all'articolo 82;
g) verifica la qualità e la sicurezza dei servizi erogati dai fornitori qualificati del SPC;
h) promuove il recepimento degli standard necessari a garantire la connettività, l'interoperabilità di base e avanzata, la cooperazione applicativa e la sicurezza del Sistema.

3. Le decisioni della Commissione sono assunte a maggioranza semplice o qualificata dei componenti in relazione all'argomento in esame. La Commissione a tale fine elabora, entro tre mesi dal suo insediamento, un regolamento interno da approvare con maggioranza qualificata dei suoi componenti.

80. *Composizione della Commissione di coordinamento del sistema pubblico di connettività.*

1. La Commissione è formata da diciassette componenti incluso il Presidente di cui al comma 2, scelti tra persone di comprovata professionalità ed esperienza nel settore, nominati con decreto del Presidente del Consiglio dei Ministri: otto componenti sono nominati in rappresentanza delle amministrazioni statali previa deliberazione del Consiglio dei Ministri, sette dei quali su proposta del Ministro per l'innovazione e le tecnologie ed uno su proposta del Ministro per la funzione pubblica; i restanti otto sono nominati su designazione della Conferenza unificata di cui all'ar-

ticolo 8 del decreto legislativo 28 agosto 1997, n. 281. Uno dei sette componenti proposti dal Ministro per l'innovazione e le tecnologie è nominato in rappresentanza della Presidenza del Consiglio dei Ministri. Quando esamina questioni di interesse della rete internazionale della pubblica amministrazione la Commissione è integrata da un rappresentante del Ministero degli affari esteri, qualora non ne faccia già parte.

2. Il Presidente del Centro nazionale per l'informatica nella pubblica amministrazione è componente di diritto e presiede la Commissione. Gli altri componenti della Commissione restano in carica per un biennio e l'incarico è rinnovabile.
3. La Commissione è convocata dal Presidente e si riunisce almeno quattro volte l'anno.
4. L'incarico di Presidente o di componente della Commissione e la partecipazione alle riunioni della Commissione non danno luogo alla corresponsione di alcuna indennità, emolumento, compenso e rimborso spese e le amministrazioni interessate provvedono agli oneri di missione nell'ambito delle risorse umane, strumentali e finanziarie disponibili a legislazione vigente, senza nuovi o maggiori oneri per la finanza pubblica.
5. Per i necessari compiti istruttori la Commissione si avvale del Centro nazionale per l'informatica nella pubblica amministrazione, di seguito denominato: «CNIPA» e sulla base di specifiche convenzioni, di organismi interregionali e territoriali.
6. La Commissione può avvalersi, nell'ambito delle risorse umane, finanziarie e strumentali disponibili a legislazione vigente, senza nuovi o maggiori oneri per la finanza pubblica, della consulenza di uno o più organismi di consultazione e cooperazione istituiti con appositi accordi ai sensi dell'articolo 9, comma 2, lettera c), del decreto legislativo 28 agosto 1997, n. 281.
7. Ai fini della definizione degli sviluppi strategici del SPC, in relazione all'evoluzione delle tecnologie dell'informatica e della comunicazione, la Commissione può avvalersi, nell'ambito delle risorse finanziarie assegnate al CNIPA a legislazione vigente e senza nuovi o maggiori oneri per la finanza pubblica, di consulenti di chiara fama ed esperienza in numero non superiore a cinque secondo le modalità definite nei regolamenti di cui all'articolo 87.

81. *Ruolo del Centro nazionale per l'informatica nella pubblica amministrazione.*

1. Il CNIPA, nel rispetto delle decisioni e degli indirizzi forniti dalla Commissione, anche avvalendosi di soggetti terzi, gestisce le risorse condivise del SPC e le strutture operative preposte al controllo e supervisione delle stesse, per tutte le pubbliche amministrazioni di cui all'articolo 2, comma 2.
2. Il CNIPA, anche avvalendosi di soggetti terzi, cura la progettazione, la realizzazione, la gestione e l'evoluzione del SPC per le amministrazioni di cui all'articolo 1, comma 1, del decreto legislativo 12 febbraio 1993, n. 39.

82. *Fornitori del Sistema pubblico di connettività.*

1. Sono istituiti uno o più elenchi di fornitori a livello nazionale e regionale in attuazione delle finalità di cui all'articolo 77.
2. I fornitori che ottengono la qualificazione SPC ai sensi dei regolamenti previsti dall'articolo 87, sono inseriti negli elenchi di competenza nazionale o regionale, consultabili in via telematica, esclusivamente ai fini dell'applicazione della disciplina di cui al presente decreto, e tenuti rispettivamente dal CNIPA a livello nazionale e dalla regione di competenza a livello regionale. I fornitori in possesso dei suddetti requisiti sono denominati fornitori qualificati SPC.
3. I servizi per i quali è istituito un elenco, ai sensi del comma 1, sono erogati, nell'ambito del SPC, esclusivamente dai soggetti che abbiano ottenuto l'iscrizione nell'elenco di competenza nazionale o regionale.
4. Per l'iscrizione negli elenchi dei fornitori qualificati SPC è necessario che il fornitore soddisfi almeno i seguenti requisiti:
   a) disponibilità di adeguate infrastrutture e servizi di comunicazioni elettroniche;
   b) esperienza comprovata nell'ambito della realizzazione gestione ed evoluzione delle soluzioni di sicurezza informatica;
   c) possesso di adeguata rete commerciale e di assistenza tecnica;

d) possesso di adeguati requisiti finanziari e patrimoniali, anche dimostrabili per il tramite di garanzie rilasciate da terzi qualificati.
5. Limitatamente ai fornitori dei servizi di connettività dovranno inoltre essere soddisfatti anche i seguenti requisiti:
   a) possesso dei necessari titoli abilitativi di cui al decreto legislativo 1° agosto 2003, n. 259, per l'ambito territoriale di esercizio dell'attività;
   b) possesso di comprovate conoscenze ed esperienze tecniche nella gestione delle reti e servizi di comunicazioni elettroniche, anche sotto il profilo della sicurezza e della protezione dei dati.

83. *Contratti quadro.*

1. Al fine della realizzazione del SPC, il CNIPA a livello nazionale e le regioni nell'ambito del proprio territorio, per soddisfare esigenze di coordinamento, qualificata competenza e indipendenza di giudizio, nonché per garantire la fruizione, da parte delle pubbliche amministrazioni, di elevati livelli di disponibilità dei servizi e delle stesse condizioni contrattuali proposte dal miglior offerente, nonché una maggiore affidabilità complessiva del sistema, promuovendo, altresì, lo sviluppo della concorrenza e assicurando la presenza di più fornitori qualificati, stipulano, espletando specifiche procedure ad evidenza pubblica per la selezione dei contraenti, nel rispetto delle vigenti norme in materia, uno o più contratti-quadro con più fornitori per i servizi di cui all'articolo 77, con cui i fornitori si impegnano a contrarre con le singole amministrazioni alle condizioni ivi stabilite.
2. Le amministrazioni di cui all'articolo 1, comma 1, del decreto legislativo 12 febbraio 1993, n. 39, sono tenute a stipulare gli atti esecutivi dei contratti-quadro con uno o più fornitori di cui al comma 1, individuati dal CNIPA. Gli atti esecutivi non sono soggetti al parere del CNIPA e, ove previsto, del Consiglio di Stato. Le amministrazioni non ricomprese tra quelle di cui al citato art. 1, comma 1, del decreto legislativo n. 39 del 1993, hanno facoltà di stipulare gli atti esecutivi di cui al presente articolo.

84. *Migrazione della Rete unitaria della pubblica amministrazione.*

1. Le Amministrazioni di cui all'articolo 1, comma 1, del decreto legislativo 12 febbraio 1993, n. 39, aderenti alla Rete unitaria della pubblica amministrazione, presentano al CNIPA, secondo le indicazioni da esso fornite, i piani di migrazione verso il SPC, da attuarsi entro diciotto mesi dalla data di approvazione del primo contratto quadro di cui all'articolo 83, comma 1, termine di cessazione dell'operatività della Rete unitaria della pubblica amministrazione.
2. Dalla data di entrata in vigore del presente articolo ogni riferimento normativo alla Rete unitaria della pubblica amministrazione si intende effettuato al SPC.

Sezione III - Rete internazionale della pubblica amministrazione e compiti del CNIPA

85. *Collegamenti operanti per il tramite della Rete internazionale delle pubbliche amministrazioni.*

1. Le amministrazioni di cui all'articolo 1, comma 1, del decreto legislativo 12 febbraio 1993, n. 39, che abbiano l'esigenza di connettività verso l'estero, sono tenute ad avvalersi dei servizi offerti dalla Rete internazionale delle pubbliche amministrazioni, interconnessa al SPC.
2. Le pubbliche amministrazioni di cui al comma 1, che dispongono di reti in ambito internazionale sono tenute a migrare nella Rete internazionale delle pubbliche amministrazioni entro il 15 marzo 2007, fatto salvo quanto previsto dall'articolo 75, commi 2 e 3.
3. Le amministrazioni non ricomprese tra quelle di cui all'articolo 1, comma 1, del decreto legislativo 12 febbraio 1993, n. 39, ivi incluse le autorità amministrative indipendenti, possono aderire alla Rete internazionale delle pubbliche amministrazioni.

86. *Compiti e oneri del CNIPA.*

1. Il CNIPA cura la progettazione, la realizzazione, la gestione ed evoluzione della Rete internazionale delle pubbliche amministrazioni, previo espletamento di procedure concorsuali ad evidenza pubblica per la selezione dei fornitori e mediante la stipula di appositi contratti-quadro secondo modalità analoghe a quelle di cui all'articolo 83.
2. Il CNIPA, al fine di favorire una rapida realizzazione del SPC, per un periodo almeno pari a due anni a decorrere dalla data di approvazione dei contratti-quadro di cui all'articolo 83, comma 1, sostiene i costi delle infrastrutture condivise, a valere sulle risorse già previste nel bilancio dello Stato.
3. Al termine del periodo di cui al comma 2, i costi relativi alle infrastrutture condivise sono a carico dei fornitori proporzionalmente agli importi dei contratti di fornitura, e una quota di tali costi è a carico delle pubbliche amministrazioni relativamente ai servizi da esse utilizzati. I costi, i criteri e la relativa ripartizione tra le amministrazioni sono determinati annualmente con decreto del Presidente del Consiglio dei Ministri, su proposta della Commissione, previa intesa con la Conferenza unificata cui all'articolo 8 del decreto legislativo 28 agosto 1997, n. 281, salvaguardando eventuali intese locali finalizzate a favorire il pieno ingresso nel SPC dei piccoli Comuni nel rispetto di quanto previsto dal comma 5.
4. Il CNIPA sostiene tutti gli oneri derivanti dai collegamenti in ambito internazionale delle amministrazioni di cui all'articolo 85, comma 1, per i primi due anni di vigenza contrattuale, decorrenti dalla data di approvazione del contratto quadro di cui all'articolo 83; per gli anni successivi ogni onere è a carico della singola amministrazione contraente proporzionalmente ai servizi acquisiti.
5. Le amministrazioni non ricomprese tra quelle di cui all'articolo 1, comma 1, del decreto legislativo 12 febbraio 1993, n. 39, che aderiscono alla Rete internazionale delle pubbliche amministrazioni, ai sensi dell'articolo 85, comma 3, ne sostengono gli oneri relativi ai servizi che utilizzano.

87. *Regolamenti.*

1. Ai sensi dell'articolo 17, comma 3, della legge 23 agosto 1988, n. 400, con uno o più decreti sulla proposta del Presidente del Consiglio dei Ministri o, per sua delega, del Ministro per l'innovazione e le tecnologie, di concerto con il Ministro per la funzione pubblica, d'intesa con la Conferenza unificata di cui all'articolo 8 del decreto legislativo 28 agosto 1997, n. 281, sono adottati regolamenti per l'organizzazione del SPC, per l'avvalimento dei consulenti di cui all'articolo 80, comma 7, e per la determinazione dei livelli minimi dei requisiti richiesti per l'iscrizione agli elenchi dei fornitori qualificati del SPC di cui all'articolo 82.

Capo IX - Disposizioni transitorie finali e abrogazioni

88. *Norme transitorie per la firma digitale.*

1. I documenti sottoscritti con firma digitale basata su certificati rilasciati da certificatori iscritti nell'elenco pubblico già tenuto dall'Autorità per l'informatica nella pubblica amministrazione sono equivalenti ai documenti sottoscritti con firma digitale basata su certificati rilasciati da certificatori accreditati.

89. *Aggiornamenti.*

1. La Presidenza del Consiglio dei Ministri adotta gli opportuni atti di indirizzo e di coordinamento per assicurare che i successivi interventi normativi, incidenti sulle materie oggetto di riordino siano attuati esclusivamente mediante la modifica o l'integrazione delle disposizioni contenute nel presente codice.

90. *Oneri finanziari.*

1. All'attuazione del presente decreto si provvede nell'àmbito delle risorse previste a legislazione vigente.

91. *Abrogazioni.*

1. Dalla data di entrata in vigore del presente testo unico sono abrogati:
   a) il decreto legislativo 23 gennaio 2002, n. 10;
   b) gli articoli 1, comma 1, lettere t), u), v), z), aa), bb), cc), dd), ee), ff), gg), hh), ii), ll), mm), nn), oo); 2, comma 1, ultimo periodo; 6; 8; 9; 10; 11; 12; 13; 14; 17; 20; 22; 23; 24; 25; 26; 27; 27-bis; 28; 28-bis; 29; 29-bis; 29-ter; 29-quater; 29-quinquies; 29-sexies; 29-septies; 29-octies; 36, commi 1, 2, 3, 4, 5 e 6; 51; del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 (Testo A);
   c) l'articolo 26, comma 2, lettere a), e), h), della legge 27 dicembre 2002, n. 289;
   d) articolo 27, comma 8, lettera b), della legge 16 gennaio 2003, n. 3;
   e) gli articoli 16, 17, 18 e 19 della legge 29 luglio 2003, n. 229.
2. Le abrogazioni degli articoli 2, comma 1, ultimo periodo, 6, commi 1 e 2; 10; 36, commi 1, 2, 3, 4, 5 e 6 del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 (Testo A), si intendono riferite anche al decreto legislativo 28 dicembre 2000, n. 443 (Testo B).
3. Le abrogazioni degli articoli 1, comma 1, lettere t), u), v), z), aa), bb), cc), dd), ee), ff), gg), hh), ii), ll), mm), nn), oo); 6, commi 3 e 4; 8; 9; 11; 12; 13; 14; 17; 20; 22; 23; 24; 25; 26; 27; 27-bis; 28; 28-bis; 29; 29-bis; 29-ter; 29-quater; 29-quinquies; 29-sexies; 29-septies; 29-octies; 51 del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 (Testo A), si intendono riferite anche al decreto del Presidente della Repubblica 28 dicembre 2000, n. 444 (Testo C).

3-bis. L'articolo 15, comma 1, della legge 15 marzo 1997, n. 59, è abrogato.

3-ter. Il decreto legislativo 28 febbraio 2005, n. 42, è abrogato.

92. *Entrata in vigore del codice.*

1. Le disposizioni del presente codice entrano in vigore a decorrere dal 1° gennaio 2006.

ARTICOLI E COMMENTI SULLA PEC

Una serie di importanti interventi, dopo la nuova spinta sull'obbligo di adottare la PEC e suoi derivati CEC, PAC, sono apparsi nella rete, citarli tutti è praticamente impossibile, avere una tabella organica di coloro che ne hanno parlato direi che è la strada da seguire. Pertanto, per tutti coloro che vogliano studiare la problematica o semplicemente ne vogliono conoscere di più in materia, la tabella in basso riporta un quadro più completo possibile dalla quale attingere le necessarie informazioni. Il prospetto include collegamenti ipertestuali ai profili degli autori, ai siti web, Blog, ai link degli scritti ed articoli sulla stampa, con note sul tipo di intervento.

Gli autori e i relativi riferimenti non hanno un ordine specifico, come pure i siti web e relativi link, sono semplicemente una raccolta di quanto è anche facilmente reperibile on-line:

Mi scuso con tutti coloro che non sono stati menzionati, ma che prego di comunicarlo, infatti, con la filosofia del "Dinamyc E-book" il testo verrà aggiornato dietro segnalazione e collaborazione dei lettori.

Autore: Massimo F. Penco
Sito Web/BLOG:
www.cittadininternet.org – www.cittadininternet.it
ARGOMENTO / NOTE:
Denuncia Unione Europea[108]
Lo Stato dell'Arte della Posta Elettronica Certificata[109]
PEC italica, pecca nostrana: "E' una manna per i criminali"[110]
DAE 2009 PEC Complicazione elettronica certificata[111]
Pec gratuita: "Cittadini di Internet" perplessi[112]

---

[108] https://www.cittadininternet.org/UserFiles/File/Proposte%20ed%20iniziative/Domanda%20congiunta%20infrazione%20UE.pdf

[109] https://www.cittadininternet.org/UserFiles/File/Pec%20o%20non%20Pec/Ad%20oltre%20un%20anno%20dall(1).pdf

[110] http://lastampa.it/_web/cmstp/tmplrubriche/tecnologia/grubrica.asp?ID_blog=30&ID_articolo=6925&ID_sezione=&sezione=

[111] https://www.cittadininternet.org/UserFiles/File/Pec%20o%20non%20Pec/PEC%20dae_1.pdf

[112] https://www.globaltrustgroup.info/userfiles/file/RASSEGNA%20STAMPA/pec-gratuita-cittadini-di-internet-perplessi.pdf

PEC: eliminata l'obbligatorietà; una vittoria di "Cittadini di Internet"[113]
Rendi sicure le tue e-mail[114]
Informatizzazione della PA: il punto non è come rispondere ma farlo[115]
Posta elettronica, e' polemica sulla gara vinta da Telecom e Poste[116]
PEC : 1 milione o 30.000[117]
Brunetta e Pec: Poste, Telecom e Postecom primi in gara[118]
PEC e obblighi di pubblicazione[119]
Brunetta annuncia la Pec per tutti da febbraio, ma i professionisti sono già in ritardo[120]
Il giallo della PEC (tra ACI e INPS)[121]
Pec Gratuita il Ministro fa flop[122]
Pec gratuita, partenza senza il botto: solo 30mila?[123]
Spaghetti Pec: al via, tra limiti e dubbi, la Posta certificata elettronica all'italiana[124]

---

113 http://www.pubblicaamministrazione.net/leggi-e-norme/news/1563/pec-eliminata-lobbligatorieta.html
114 https://www.globaltrustgroup.info/userfiles/file/RASSEGNA%20STAMPA/026-028.pdf
115 https://www.globaltrustgroup.info/userfiles/file/RASSEGNA%20STAMPA/Informatizzazione%20della%20PA_il%20punto_non_come_rispondere_ma_farlo_AgoraVox_Italia.pdf
116 https://www.globaltrustgroup.info/userfiles/file/RASSEGNA%20STAMPA/Voce%20-%20Posta%20elettronica,%20e'%20polemica%20sulla%20gara%20vinta%20da%20Telecom%20e%20Poste.pdf
117 https://www.globaltrustgroup.info/userfiles/file/RASSEGNA%20STAMPA/PEC_%201%20milione%20o%2030%20mila_Office_World.pdf
118 https://www.globaltrustgroup.info/userfiles/file/RASSEGNA%20STAMPA/Brunetta%20e%20Pec_%20Poste,%20Telecom%20e%20Postecom%20primi%20in%20gara%20-%20Notizie%20-%20ITespresso_it.pdf
119 https://www.globaltrustgroup.info/userfiles/file/RASSEGNA%20STAMPA/metromagazine_%20PEC%20e%20obblighi%20di%20pubblicazione.pdf
120 https://www.globaltrustgroup.info/userfiles/file/RASSEGNA%20STAMPA/Brunetta%20annuncia%20la%20Pec%20per%20tutti%20da%20febbraio,%20ma%20i%20professionisti%20sono%20gi%EF%BF%BD%20in%20ritardo%20_%20BitCity%20_%20La%20citta%20della%20tecnologia.pdf
121 https://www.globaltrustgroup.info/userfiles/file/RASSEGNA%20STAMPA/pec_richiedila_allaccio.pdf
122 https://www.globaltrustgroup.info/userfiles/file/RASSEGNA%20STAMPA/i-dome_com%20-%20PEC%20gratuita_%20Il%20Ministro%20fa%20flop.pdf
123 https://www.globaltrustgroup.info/userfiles/file/RASSEGNA%20STAMPA/pec_gratuita__parte.pdf

"Pec" di Stato gratuita? In realtà costa cara[125]
Brunetta: Dieci milioni di Pec gratis entro il 2010[126]
Pec, i conti non tornano: 200.000 o 70.000? Il contatore smentisce Brunetta[127]
OMAT REPORT Cronaca di una incursione[128]

Autore: Marco Scialdone
Sito Web/BLOG:
http://scialdone.blogspot.com/
ARGOMENTO / NOTE:
La Posta Elettronica Certificata Quadro normativo di riferimento[129]

Autore: Guido Scorza
Sito Web/BLOG:
www.guidoscorza.it
ARGOMENTO / NOTE:
PEC: comunicare è diverso da firmare…e l'identità è una cosa seria[130]
PEC: sia fatta la volontà del Ministro[131]
Pec(che)?[132]
Innovazione fa rima con contraddizione?[133]
Fermate quella PEC(icchina)![134]
PEC e pubblica amministrazione, i sospetti di un bando poco chiaro[135]

---

[124] https://www.globaltrustgroup.info/userfiles/file/RASSEGNA%20STAMPA/pec_al_via_fra_mille_dubbi.PDF
[125] http://www.lastampa.it/_web/cmstp/tmplrubriche/tecnologia/grubrica.asp?ID_blog=30&ID_articolo=6525&ID_sezione=38&sezione=News
[126] http://www.itespresso.it/brunetta-dieci-milioni-di-pec-gratis-entro-il-2010-41561.html
[127] http://www.ilsalvagente.it/Sezione.jsp?titolo=Pec%2C+i+conti+non+tornano%3A+200.000+o+70.000%3F+Il+contatore+smentisce+Brunetta&idSezione=6997
[128] http://www.cittadininternet.it/?p=900
[129] http://computerlaw.files.wordpress.com/2009/10/la-posta-elettronica-certificata.pdf
[130] http://www.guidoscorza.it/?p=978
[131] http://www.guidoscorza.it/?p=1021
[132] http://www.guidoscorza.it/?p=1127
[133] http://punto-informatico.it/2719055/PI/Commenti/innovazione-fa-rima-contraddizione.aspx
[134] http://www.guidoscorza.it/?p=1162#comment-45623
[135] http://www.hostingtalk.it/news/mercato-italiano/4727/pec-e-pubblica-amministrazione-i-sospetti-di-un-bando-poco-chiaro

E-mail Pec per tutti i cittadini per dialogare con la pubblica amministrazione. Alcune interessanti considerazioni[136]
PEC: guarda come di spartisco il mercato ed accontento tutti![137]

Autore: Michele Iaselli
Sito Web/BLOG:
www.micheleiaselli.it
ARGOMENTO / NOTE:
Un sondaggio sulla PEC[138]

Autore: Pino Bruno
Sito Web/BLOG:
www.pinobruno.it
ARGOMENTO / NOTE:
La Posta Elettronica Certificata è un'altra brutta storia italiana[139]
La PEC "gratuita" ci costerà almeno 50 milioni di euro[140]

Autore: Andrea Lisi
Sito Web/BLOG:
http://www.scintlex.it - www.studiolegalelisi.it
ARGOMENTO / NOTE:
PEC-CHÈ? Ovvero le continue novità legislative in tema di Posta Elettronica Certificata e l'avvilito sconcerto dello studioso del diritto![141]
PEC e CEC PAC: Troppa Burocrazia e Regole poco chiare[142]
E' un regalo o un CEC-PAC-co?[143]
Digitalizzazione documentale, che fine fa la PEC?[144]

---

136 http://www.webmasterpoint.org/approfondimenti/approfondimenti/diritto/ministro-brunetta-regala-posta-elettronica-certificata.html
137 http://www.guidoscorza.it/?p=943
138 http://micheleiaselli.blogspot.com/2009/07/un-sondaggio-sulla-pec.html
139 http://www.pinobruno.it/2009/07/la-posta-elettronica-certificata-e-unaltra-brutta-storia-italiana/
140 http://www.pinobruno.it/2009/08/la-pec-gratuita-ci-costera-almeno-50-milioni-di-euro/
141 http://www.scintlex.it/notizia/362/169.html
142 http://www.studiolegalelisi.it/notizia.php?titolo_mod=278_PEC_e_CEC_PAC__Troppa_Burocrazia_e_Regole_poco_chiare.html
143 http://www.studiolegalelisi.it/notizia.php?titolo_mod=236_E%92_un_regalo_o_un_CEC-PAC-co_.html

Sodoma e i sette peccati normativi in materia di digitalizzazione[145]
La Pec nei concorsi Pubblici[146]
La tecnologia governa il diritto nella P.A. Digitale?[147]

Autore: Valentino Spataro
Sito Web/BLOG:
www.civile.it
ARGOMENTO / NOTE:
La firma elettronica italiana e' una delle aberrazioni peggiori. Sempre invocata, mai decollata[148]

Autore: Francesco Forestiero
Sito Web/BLOG:
ARGOMENTO / NOTE:
Da PEC a CEC-PAC: un'evoluzione?[149]
Pec Pac Puc Pic Splat[150]!

Il Sole 24 Ore
La mail certificata convince i commercialisti[151]

I-Dome www.I-dome.com di Massimo F. Penco
Considerazioni e critiche sul Nuovo Codice dell'Amministrazione Digitale *"Morto un Cad se ne fa sempre un altro"*
CITAZIONI
Ho ritenuto opportuno dare al lettore un'ampia panoramica alle citazioni in questo mio libro, per dare un'idea di quanto ci sia nel mondo della rete di informazioni su alcuni specifici argomenti e

[144] http://punto-informatico.it/2527018/PI/Commenti/digitalizzazione-documentale-che-fine-fa-pec.aspx
[145] http://punto-informatico.it/2693405/PI/Commenti/sodoma-sette-peccati-normativi-materia-digitalizzazione.aspx
[146] http://saperi.forumpa.it/story/50991/lutilizzo-della-pec-nei-concorsi-pubblici-commento-alla-circolare-n-122010
[147] http://www.studiolegalelisi.it/notizia.php?titolo_mod=312_La_tecnologia_governa_il_diritto_nella_P.A._Digitale
[148] http://www.civile.it/internet/visual.php?num=69387
[149] http://www.techblogs.it/office/2009/09/da-pec-a-cecpac-unevoluzione.html
[150] http://allarovescia.blogspot.com/2009/10/pec-pac-puc-pic-splat.html
[151] http://www.cittadininternet.org/UserFiles/File/Pec%20o%20non%20Pec/il%20solepec.pdf

quanto si sia scritto su di essi, in modo che, chi lo desidera, potrà arricchire la propria conoscenza.

Penso che molti di voi ne rimarranno sbalorditi e pensare che questa mia lista è tutt'altro che esaustiva, per sincerarsene ad esempio, è sufficiente digitare in libri di Google: *"e-mail are like postcard"* rimarrete sorpresi nel vedere quanti autori hanno trattato questa materia, ben oltre quelli sotto elencati.

Pag. 191 *La Posta Elettronica è come una cartolina postale. "e-mail are like postcard"*

1. *Security Awareness: Applying Practical Security in Your World*[152] *by Mark Ciampa*[153] *pag. 126*
2. *E-Mail Rules: A Business Guide to Managing Policies, Security, and Legal Issues for E-Mail and Digital Communication*[154] *by Nancy Flynn*[155]*, Randolph Kahn*[156] *pag 173*
3. *Handbook of information security by Hossein Bidgoli*[157] *pag. 574*
4. *Hot Marketing, Cool Profits by Roger Brooksbank*[158] *pag. 111*
5. *Understanding Computers: Today and Tomorrow*[159] *by Deborah Morley pag. 367*
6. *Understanding Computers in a Changing Society*[160] *by Deborah Morley pag. 147*
7. *Web 101*[161] *By Wendy G. Lehnert, Richard Kopec*
8. *Protect Your Privacy: How **to** Protect Your Identity as Well as Your by Duncan Long pag. 164*
9. *PGP: pretty good privacy*[162] *by Simson Garfinke pag. 9*
10. *Cybersins and digital good deeds: a book about technology and ethics*[163] *by Mary Ann Bell, Bobby Ezell, James L. Van Roekel pag. 29*

---

[152] http://www.goodreads.com/book/show/2563914.Security_Awareness
[153] http://www.goodreads.com/author/show/317868.Mark_Ciampa
[154] http://www.amazon.com/gp/product/0814471889/ref=cm_rdp_product
[155] http://www.google.it/search?tbs=bks:1&tbo=p&q=+inauthor:%22Nancy+Flynn%22
[156] http://www.google.it/search?tbs=bks:1&tbo=p&q=+inauthor:%22Randolph+Kahn%22
[157] http://www.google.it/search?tbs=bks:1&tbo=p&q=+inauthor:%22Hossein+Bidgoli%22
[158] http://www.google.it/search?tbs=bks:1&tbo=p&q=+inauthor:%22Roger+Brooksbank%22
[159] http://books.google.it/books?id=0BXAYiG-Ts8C&pg=PA367&dq=email+are+like+postcard&hl=it&ei=t3FVTIe0NYuPsAbv2JjiAQ&sa=X&oi=book_result&ct=result&resnum=7&ved=0CEoQ6AEwBg
[160] http://books.google.it/books?id=aonxxWg4u4cC&pg=PA147&dq=email+are+like+postcard&hl=it&ei=t3FVTIe0NYuPsAbv2JjiAQ&sa=X&oi=book_result&ct=result&resnum=8&ved=0CE8Q6AEwBw
[161] http://books.google.it/books?id=Tc_ZAAAAMAAJ&q=email+are+like+postcard&dq=email+are+like+postcard&hl=it&ei=t3FVTIe0NYuPsAbv2JjiAQ&sa=X&oi=book_result&ct=result&resnum=10&ved=0CFkQ6AEwCQ
[162] http://books.google.it/books?id=cSe_0OnZqjAC&pg=PA9&dq=email+are+like+postcard&hl=it&ei=nHpVTKPJLp-psQbyzdniAQ&sa=X&oi=book_result&ct=result&resnum=5&ved=0CD4Q6AEwBDgK
[163] http://books.google.it/books?id=nqM_S9uAE9IC&pg=PA129&dq=email+are+like+postcard&hl=it&ei=nHpVTKPJLp-psQbyzdniAQ&sa=X&oi=book_result&ct=result&resnum=6&ved=0CEMQ6AEwBTgK

11. *Taming the **E-mail** Tiger: **E-mail** Management for Compliance*[164], *by Robert F. Smallwood pag. 53*
12. *Open source solutions for small business problems*[165] *by John Locke pag. 104*

BIBLIOGRAFIA

- Wikipedia Wikimedia Foundation, Inc.[166]
- **Altalex** Quotidiano scientifico di informazione giuridica
- Michele Robotti Tratto dal Libro "La PEC Posta Elettronica Certificata" di Emilio Robotti **COLLANA INFORMATICA GIURIDICA** diretta da Michele Iaselli edita da Altalex
- Bidgoli, H. (2009). *The Internet.* John Wiley & Sons, Inc.
- Microsoft Librerie Supporto Tecnico

[164] http://books.google.it/books?id=6Q0voyWUf0EC&pg=PA53&dq=email+are+like+postcard&hl=it&ei=nHpVTKPJLp-psQbyzdniAQ&sa=X&oi=book_result&ct=result&resnum=7&ved=0CEgQ6AEwBjgK

[165] http://books.google.it/books?id=76Q2Z3fcgJIC&pg=PA104&dq=email+are+like+postcard&hl=it&ei=nHpVTKPJLp-psQbyzdniAQ&sa=X&oi=book_result&ct=result&resnum=9&ved=0CFIQ6AEwCDgK

[166] http://www.wikimediafoundation.org/

LA POSTA ELETTRONICA TECNICA & BEST PRACTICE vuole essere una guida per tutti coloro che usano ogni giorno la posta elettronica e vogliono approfondire ed impiegare in modo esaustivo questo mezzo di comunicazione . E' una pubblicazione di tipo divulgativo, ma ricca di approfondimenti tecnici pratici e giuridici.

Massimo F. Penco Da sempre impegnato direttamente o indirettamente nella sicurezza informatica, delle reti, comunicazioni e sistemi. Ha viaggiato in tutto il Mondo ricoprendo cariche direttive, anche come consulente, per importanti istituzioni finanziarie, industrie e governi di vari paesi, Stati Uniti, Regno Unito. Forse uno dei maggiori esperti nel mondo in questo campo. Consulente e ricercatore di computer crime, sicurezza dei sistemi di comunicazione e reti informatiche, giornalista internazionale e scrittore di questa materia; animatore di congressi a livello mondiale, autore di numerosi articoli sul tema. Già consulente dei Lloyd's di Londra, dell'associazione bancaria italiana, membro del comitato di automazione bancaria ABI, consulente dell'FBI, membro dell'Institute of Electronic Engineers USA, del Computer Security Institute della National Computer Security Association, dell'American Chamber of Commerce in Italy, dell'American Academy of Forensic Sciences ed altre associazioni internazionali, Presidente e fondatore di Cittadini di Internet.
PHD Dr. In ingegneria elettronica all'università di Stanford, master in security technology and risk management presso lo Stanford Research Institute.
Una lunga carriera professionale , associativa e didattica con ultimi incarichi in aziende leader del settore, già direttore per l'Europa di Verisign, oggi Vice Presidente Emea del Gruppo Comodo, Docente e titolare di master in università, in Italia ed all'estero.